Dimension ES-4024

Ethernet Switch

March 2004

Version 3.50

User's Guide

ZyXEL
Unleash Networking Power

Copyright

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two (2) years from the date of purchase. During the warranty period and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind of character to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Interference Statements and Warnings

FCC Interference Statement

This switch complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:

(1) This switch may not cause harmful interference.

(2) This switch must accept any interference received, including interference that may cause undesired operations.

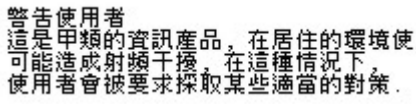
FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital switch, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning:

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Taiwanese BSMI (Bureau of Standards, Metrology and Inspection) A Warning:



Certifications

Refer to the product page at www.zyxel.com.

Customer Support

If you have questions about your ZyXEL product or desire assistance, contact ZyXEL Communications Corporation offices worldwide, in one of the following ways:

Contacting Customer Support

When you contact your customer support representative, have the following information ready:

- Product model and serial number.
- Firmware version information.
- Warranty information.
- Date you received your product.
- Brief description of the problem and the steps you took to solve it.

METHOD / LOCATION	SUPPORT E-MAIL SALES E-MAIL	TELEPHONE[1] FAX[1]	WEB SITE FTP SITE	REGULAR MAIL
WORLDWIDE	support@zyxel.com.tw sales@zyxel.com.tw	+886-3-578-3942 +886-3-578-2439	www.zyxel.com www.europe.zyxel.com ftp.zyxel.com ftp.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
NORTH AMERICA	support@zyxel.com sales@zyxel.com	+1-800-255-4101 +1-714-632-0882 +1-714-632-0858	www.us.zyxel.com ftp.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
GERMANY	support@zyxel.de sales@zyxel.de	+49-2405-6909-0 +49-2405-6909-99	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
FRANCE	info@zyxel.fr	+33 (0)4 72 52 97 97 +33 (0)4 72 52 19 20	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
SPAIN	support@zyxel.es sales@zyxel.es	+34 902 195 420 +34 913 005 345	www.zyxel.es	ZyXEL Communications Alejandro Villegas 33 1º, 28043 Madrid Spain
DENMARK	support@zyxel.dk sales@zyxel.dk	+45 39 55 07 00 +45 39 55 07 07	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 5 2860 Soeborg Denmark
NORWAY	support@zyxel.no sales@zyxel.no	+47 22 80 61 80 +47 22 80 61 81	www.zyxel.no	ZyXEL Communications A/S Nils Hansens vei 13 0667 Oslo Norway
SWEDEN	support@zyxel.se sales@zyxel.se	+46 31 744 7700 +46 31 744 7701	www.zyxel.se	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
FINLAND	support@zyxel.fi	+358-9-4780-8411	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland

[1] "+" is the (prefix) number you enter to make an international telephone call.

Table of Contents

List of Figures

List of Tables

Preface

Congratulations on your purchase from the Dimension series of Ethernet switches.

This preface introduces you to the ES-4024 and discusses the conventions of this User's Guide. It also provides information on other related documentation.

About the ES-4024

There are two ES-4024 models. The ES-4024 DC model requires DC power supply input of -48 VDC to -60 VDC, 1.84A Max. The ES-4024 AC model requires 100~240VAC/1.5A power.

All figures in this guide display the ES-4024 AC model unless specifically noted otherwise.

The ES-4024 Ethernet switch is a layer 3 managed switch with features ideally suited in any environment with unshielded twisted pair (UTP) wiring. It can deliver broadband IP services to:

- Multi-tenant unit (MTU) buildings (hotels, motels, resorts, residential multi-dwelling units, office buildings, educational establishments, etc.)
- Public facilities (convention centers, airports, plazas, train stations, etc.)
- Enterprises.

It can also be deployed as a mini-POP (point-of-presence) in a building basement delivering 10/100Mbps data service over Category 5 wiring to each customer.

General Syntax Conventions

- This guide shows you how to configure the switch using the web configurator and CLI commands. See the online HTML help for information on individual web configurator screens.
- Mouse action sequences are denoted using a comma. For example, click **Start, Settings, Control Panel, Network** means first you click **Start**, click or move the mouse pointer over **Settings**, then click or move the mouse pointer over **Control Panel** and finally click (or double-click) **Network**.
- "Enter" means for you to type one or more characters. "Select" or "Choose" means for you to use one of the predefined choices.
- Predefined choices are in **Bold Arial** font.
- Button and field labels, links and screen names in are in **Bold Times New Roman** font.
- For brevity's sake, we will use "e.g." as shorthand for "for instance", and "i.e." as shorthand for "that is" or "in other words" throughout this manual.
- The ES-4024 Ethernet Switch may be referred to as "the ES-4024", "the ES", or, simply, as "the switch" in this guide.

Graphics Icons Key

 The ES	 Switch	 Server
 Computer	 Printer	 Gateway

Related Documentation

Web Configurator Online HTML help

The online HTML help shows you how to use the web configurator to configure individual screens. More background information can be found in this UG.

ZyXEL Web Site

The ZyXEL download library at www.zyxel.com contains additional support documentation as well as an online glossary of networking terms.

User Guide Feedback

Help us help you. E-mail all User Guide-related comments, questions or suggestions for improvement to techwriters@zyxel.com.tw or send regular mail to The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Thank you.

Part I

Features And Applications

This part acquaints you with the features and applications of the ES-4024.

Chapter 1
Getting to Know the ES-4024

This chapter describes the key features, benefits and applications of the ES-4024.

The ES-4024 is a stand-alone layer 3 Ethernet switch with 24 10/100Mbps ports, two GBIC slots and one slot for a stacking module.

With its built-in web configurator, managing and configuring the switch is easy. From cabinet management to port-level control and monitoring, you can visually configure and manage your network via the web browser. Just click your mouse instead of typing cryptic command strings. In addition, the switch can also be managed via Telnet, the console port, or third-party SNMP management.

1.1 Features

The next two sections describe the main hardware and firmware features of the ES-4024.

1.1.1 Hardware Features

Power

The ES-4024 DC model requires DC power supply input of -48 VDC to -60 VDC, 1.84A Max. The ES-4024 AC model requires 100~240VAC/1.5A power.

24 10/100 Mbps Fast Ethernet Ports

Connect up to 24 computers or switches to the 10/100Mbps auto-negotiating, automatic cable sensing (auto-MDIX) Ethernet RJ-45 ports. All Ethernet ports support

- IEEE 802.3/3u/3z/3ab standards
- Back pressure flow control in half duplex mode
- IEEE 802.3x flow control in full duplex mode

Two GBIC Slots for Uplink Modules

The modules allow the ES-4024 to connect to another WAN switch or daisy-chain to other switches.

One Slot for Stacking Module

Up to eight switches may be stacked using a stacking module.

Console Port

Use the console port for local management of the switch.

Fans

The fans cool the ES-4024 sufficiently to allow reliable operation of the switch in even poorly ventilated rooms or basements.

1.1.2 Firmware Features

Layer 2 Features

- 16K MAC address table
- Broadcast storm control
- 12.8Gbps switching fabric capacity
- Spanning Tree Protocol (IEEE 802.1d) with rapid switch failure recognition and recovery (IEEE 802.1w)
- Support port-based VLAN and tag-based VLAN (IEEE 802.1Q, up to 4K VLANs)
- GVRP support for dynamic VLAN registration
- Port mirroring
- IGMP snooping

Layer 3 Features

- Wire speed IP forwarding
- 16K IP address table
- Supports static routing
- Supports RIP (version 1 and version 2)
- Supports OSPF version 2
- Support up to 64 IP routing domains
- DHCP relay/server
- IGMP
- VRRP (RFC 2338)
- DiffServ DSCP with TOS to IEEE 802.1p mapping
- DVMRP

Management

- Web configurator
- Command-line interface locally via console port or remotely via Telnet
- SNMP
    - RFC1213 MIB II
    - RFC2011 IP MIB
    - RFC1493 Bridge MIB
    - RFC1643 Ethernet MIB
    - RFC1757 four groups of RMON
    - RFC2674 VLAN MIB

System Monitoring

- System status (link status, rates, statistics counters)
- SNMP
- Temperatures, voltage, fan speed reports and alarms
- Port Mirroring allows you to analyze one port's traffic from another

Security

- System management password protection
- IEEE 802.1Q VLAN
- Port-based VLAN
- IEEE 802.1x port-based authentication
- Static MAC/IP address filtering
- Limit dynamic port MAC address learning
- Filtering based on source/destination IP addresses

Port Link Aggregation

The ES-4024 adheres to the IEEE 802.3ad standard for static and dynamic port link aggregation

Bandwidth Control

- The ES supports rate limiting in 1Kbps increments allowing you to create different service plans
- The ES supports IGMP snooping enabling group multicast traffic to be only forwarded to ports that are members of that group; thus allowing you to significantly reduce multicast traffic passing through your switch

Quality of Service

- Four priority queues so you can ensure mission-critical data gets delivered on time
- Follows the IEEE 802.1p priority setting standard based on source/destination MAC/IP addresses
- Support RFC 2475 DiffServ
- Support traffic priority based on the TCP/UDP ports

STP (Spanning Tree Protocol) / RSTP (Rapid STP)

(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a switch to interact with other (R)STP -compliant switches in your network to ensure that only one path exists between any two stations on the network.

1.2 Applications

This section shows a few examples of using the ES-4024 in various network environments.

1.2.1 Backbone Application

In this application, the switch is an ideal solution for small networks where rapid growth can be expected in the near future.

The switch can be used standalone for a group of heavy traffic users. You can connect computers directly to the switch's port or connect other switches to the ES-4024.

In this example, all computers connected directly or indirectly to the ES-4024 can share super high-speed applications on the server.

To expand the network, simply add more networking devices such as switches, routers, computers, print servers etc.

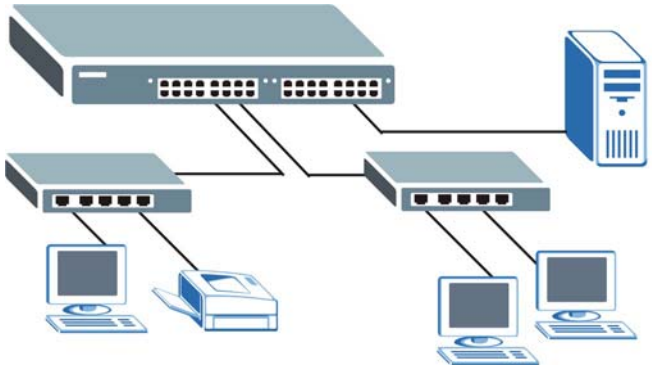


Figure 1-1 Backbone Application

1.2.2 Bridging Example

In this example application the switch is the ideal solution for different company departments to connect to the corporate backbone. It can alleviate bandwidth contention and eliminate server and network bottlenecks. All users that need high bandwidth can connect to high-speed department servers via the switch. You can provide a super-fast uplink connection by using a GBIC module on the ES-4024.

Moreover, the switch eases supervision and maintenance by allowing network managers to centralize multiple servers at a single location.

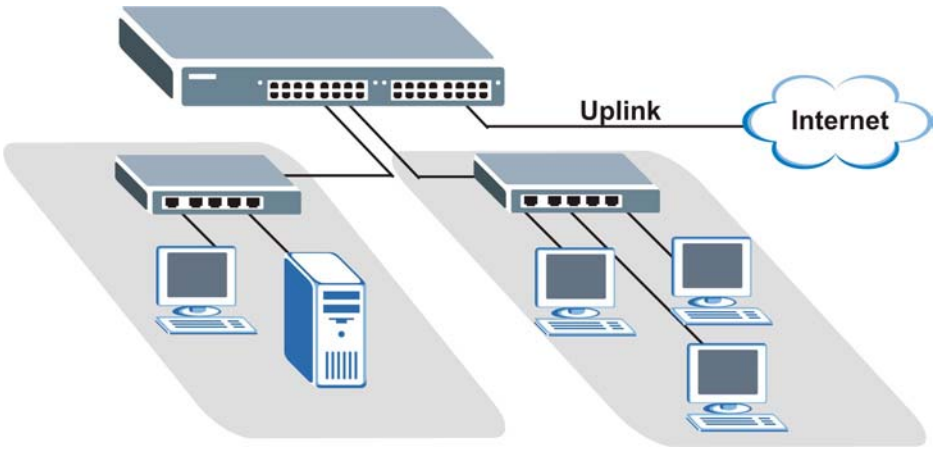


Figure 1-2 Bridging Application

Full-duplex mode operation only applies to point-to-point access (for example, when attaching the switch to a workstation, server, or another switch). When connecting to hubs, use a standard cascaded connection set at half-duplex operation.

1.2.3 High Performance Switched Workgroup Example

The switch is ideal for connecting two power workgroups that need high bandwidth. In the following example, use trunking to connect these two power workgroups.

Switching to higher-speed LANs such as FDDI or ATM is not feasible for most people due to the expense of replacing all existing Ethernet cables and adapter cards, restructuring your network and complex maintenance.

The ES-4024 can provide the same bandwidth as FDDI and ATM at much lower cost while still being able to use existing adapters and switches. Moreover, the current LAN structure can be retained as all ports can freely communicate with each other.

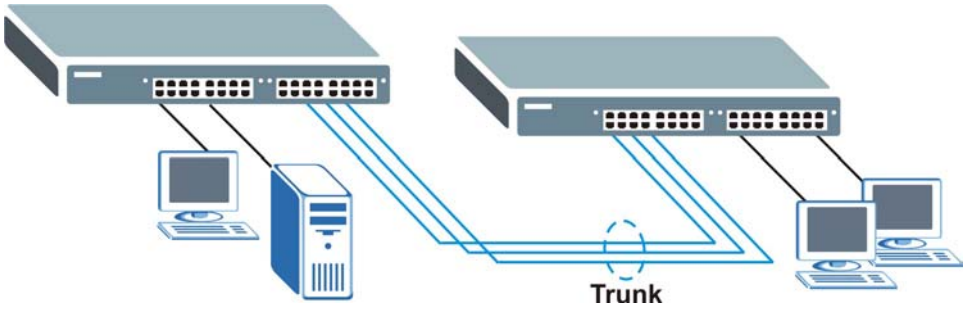


Figure 1-3 High Performance Switched Workgroup Application

1.2.4 IEEE 802.1Q VLAN Application Examples

This section shows a workgroup and a shared server example using 802.1Q tagged VLANs. For more information on VLANs, see the *Switch Setup* section and the *VLAN* chapter in this User's Guide. A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Stations on a logical network

belong to one group. A station can belong to more than one group. With VLAN, a station cannot directly talk to or hear from stations that are not in the same group(s) unless such traffic first goes through a router.

Tag-based VLAN Workgroup Example

Ports in the same VLAN group share the same broadcast domain thus increase network performance through reduced broadcast traffic. VLAN groups can be modified at any time by adding, moving or changing ports without any re-cabling.

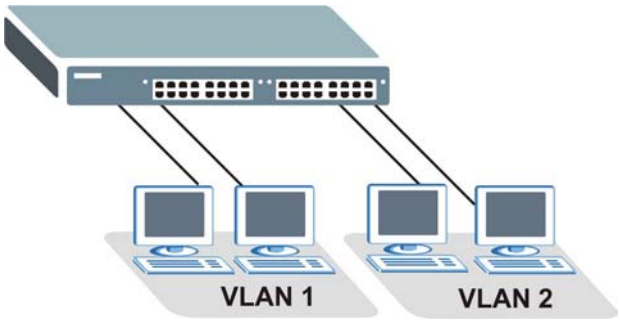


Figure 1-4 VLAN Workgroup Application

VLAN Shared Server Example

Shared resources such as a server can be used by all ports in the same VLAN as the server, as shown in the following example. In this example, only ports that need access to the server need belong to VLAN 3 while they can belong to other VLAN groups too.

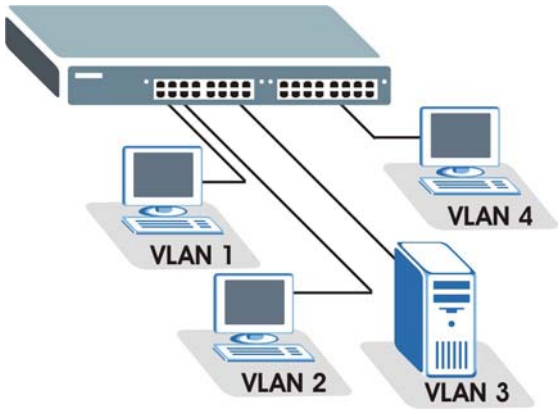


Figure 1-5 Shared Server Using VLAN Example

Part II

Hardware Installation and Connections

This part acquaints you with installation scenarios of the ES, instructs you on how to make the hardware connections including installing/removing modules, shows some stacking/uplink examples and explains the front panel LEDs.

Chapter 2
Hardware Installation

This chapter shows two switch installation scenarios.

2.1 Installation Scenarios

The switch can be placed on a desktop or rack-mounted on a standard EIA rack. Use the rubber feet in a desktop installation and the brackets in a rack-mounted installation.

For proper ventilation, allow at least 4 inches (10 cm) of clearance at the front and 3.4 inches (8 cm) at the back of the switch. This is especially important for enclosed rack installations.

2.1.1 Desktop Installation Procedure

Step 1. Make sure the switch is clean and dry.

Step 2. Set the switch on a smooth, level surface strong enough to support the weight of the switch and the connected cables. Make sure there is a power outlet nearby.

Step 3. Make sure there is enough clearance around the switch to allow air circulation and the attachment of cables and the power cord.

Step 4. Remove the adhesive backing from the rubber feet.

Step 5. Attach the rubber feet to each corner on the bottom of the switch. These rubber feet help protect the switch from shock or vibration and ensure space between switches when stacking.

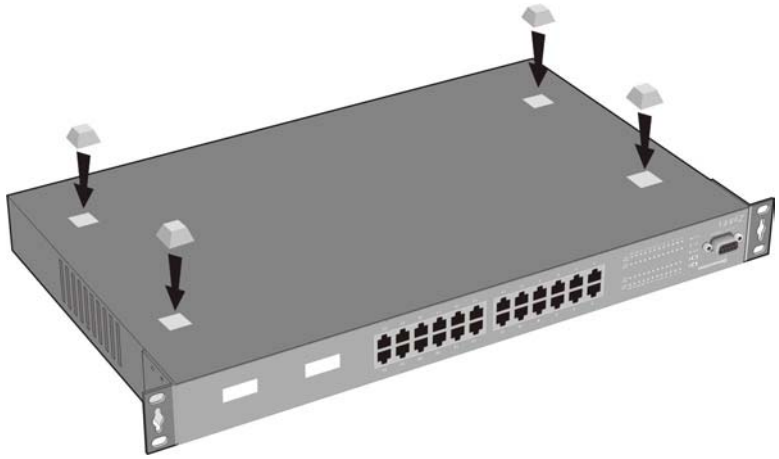


Figure 2-1 Attaching Rubber Feet

Do not block the ventilation holes. Leave space between switches when stacking.

2.1.2 Rack-Mounted Installation

The switch can be mounted on an EIA standard size, 19-inch rack or in a wiring closet with other equipment. Follow the steps below to mount your switch on a standard EIA rack using a rack-mounting kit.

Step 1. Align one bracket with the holes on one side of the switch and secure it with the bracket screws smaller than the rack-mounting screws. Similarly, attach the other bracket.

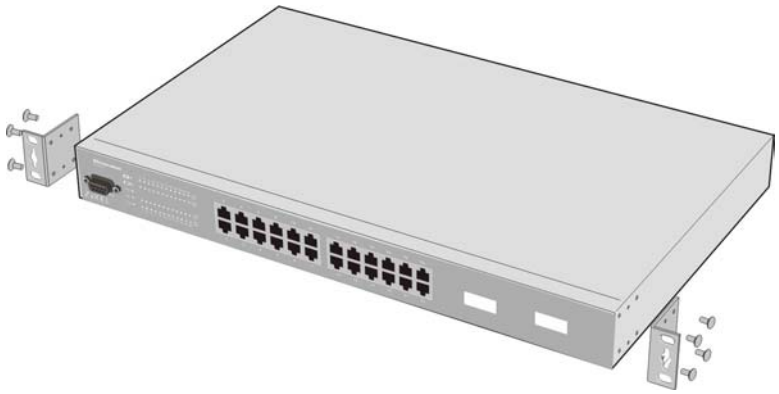


Figure 2-2 Attaching Mounting Brackets and Screws

Step 2. After attaching both mounting brackets, position the switch in the rack by lining up the holes in the brackets with the appropriate holes on the rack. Secure the switch to the rack with the rack-mounting screws.

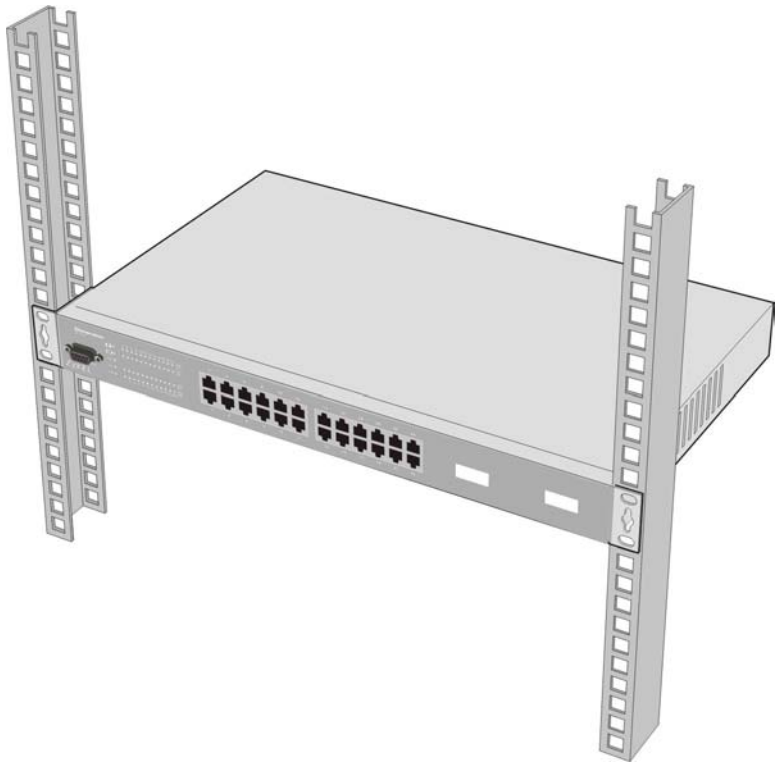


Figure 2-3 Mounting the ES to an EIA standard 19-inch rack

Chapter 3
Hardware Connections

This chapter acquaints you with the front and rear panels, shows you how to make the connections, install/remove (optional) modules and explains the LEDs.

3.1 Safety Warnings

- The length of exposed (bare) power wire should not exceed 7mm.
- Do not use this product near water, for example, in a wet basement.
- Only a qualified technician should service or disassemble this device.

3.2 Front Panel

The following figure shows the front panel of the ES-4024. The front panel contains a console port for local switch management, switch LEDs, 24 RJ-45 Ethernet ports and two GBIC (3.3V) slots for uplink modules.

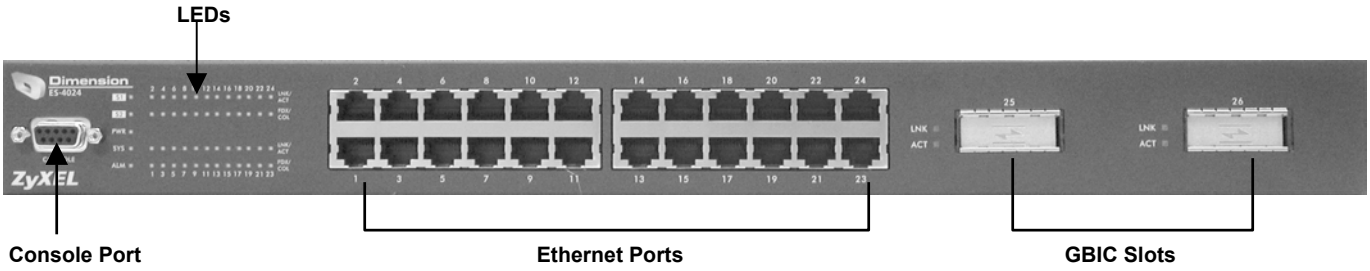


Figure 3-1 ES-4024 Front Panel

The following table describes the front panel port connections.

Table 3-1 ES-4024 Front Panel

CONNECTOR	DESCRIPTION
Console Port	The console port is for local configuration of the ES-4024.
24 10/100 Mbps RJ-45 Ethernet Ports	Connect these ports to a computer, a hub, an Ethernet switch or router.
GBIC Slots	For gigabit uplink modules.

3.2.1 Console Port

For local management, you can use a computer with terminal emulation software configured to the following parameters:

- VT100 terminal emulation
- 9600 bps
- No parity, 8 data bits, 1 stop bit
- No flow control

Connect the male 9-pin end of the console cable to the console port of the ES-4024. Connect the female end to a serial port (COM1, COM2 or other COM port) of your computer.

3.2.2 Ethernet Ports

The ES-4024 has 24 10/100Mbps auto-negotiating, auto-crossover Ethernet ports. In 10/100Mbps Fast Ethernet, the speed can be 10Mbps or 100Mbps and the duplex mode can be half duplex or full duplex.

When auto-negotiation is turned on, an Ethernet port on the ES-4024 negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer Ethernet port does not support auto-negotiation or turns off this feature, the ES-4024 determines the connection speed by detecting the signal on the cable and using half duplex mode. When the ES-4024's auto-negotiation is turned off, an Ethernet port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer Ethernet port are the same in order to connect.

Default Ethernet Settings

The factory default negotiation settings for the Ethernet ports on the ES-4024 are:

- Speed: Auto
- Duplex: Auto
- Flow control: on

Auto-crossover

All ports are auto-crossover, that is auto-MDIX ports (Media Dependent Interface Crossover), so you may use either a straight-through Ethernet cable or crossover Ethernet cable for all Ethernet port connections. Auto-crossover ports automatically sense whether they need to function as crossover or straight ports, so crossover cables can connect both computers and switches/hubs.

3.3 Stacking Module

LEDs in the (optional) stacking modules and module hardware installation steps are described in the corresponding module manual.

3.4 Rear Panel

The following figure shows the rear panel of the ES-4024. The rear panel contains the slot for the stacking module and the power receptacle. Refer to the module manual for descriptions on hardware installation.

Figure 3-2 ES-4024 Rear Panel: AC model

Figure 3-3 ES-4024 Rear Panel: DC Model

3.4.1 Power Connector

Make sure you are using the correct power source as shown on the panel.

To connect the power to the ES-4024 AC unit, insert the female end of power cord to the power receptacle on the rear panel. Connect the other end of the supplied power cord to a 100~240VAC/1.5A power outlet. Make sure that no objects obstruct the airflow of the fans (located on the side of the unit).

The ES-4024 DC unit requires DC power supply input of –48 VDC to -60 VDC, 1.84A Max. To connect the power to the unit, insert the one end of the supplied power cord to the power receptacle on the rear panel and the other end to a power outlet.

3.5 Front Panel LEDs

After you connect the power to the switch, view the LEDs to ensure proper functioning of the switch and as an aid in troubleshooting. The front panel LEDs are as follows.

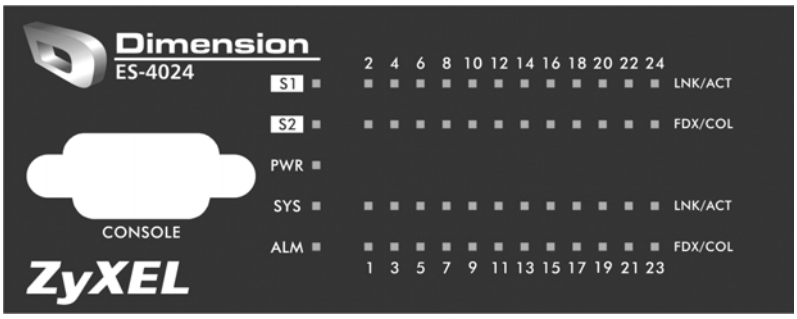


Figure 3-4 Front Panel LEDs

The following table describes the LED indicators on the front panel of the ES-4024.

Table 3-2 Front Panel: LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
S1	Green	Blinking	The system is transmitting/receiving through the stacking port.
S2		ON	The link through the stacking port is up.
		OFF	The link through the stacking port is down.
PWR	Green	ON	The system is turned on.
		OFF	The system is off.

Table 3-2 Front Panel: LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
SYS	Green	Blinking	The system is rebooting and performing self-diagnostic tests.
		ON	The system is on and functioning properly.
		OFF	The power is off or the system is not ready/malfunctioning.
ALM	Red	ON	There is a hardware failure.
		OFF	The system is functioning normally.
LNK/ACT (Ethernet ports)	Green	Blinking	The system is transmitting/receiving to/from a 10 Mbps Ethernet network.
		ON	The link to a 10 Mbps Ethernet network is up.
		OFF	The link to a 10 Mbps Ethernet network is down.
	Amber	Blinking	The system is transmitting/receiving to/from a 100 Mbps Ethernet network.
		ON	The link to a 100 Mbps Ethernet network is up.
		OFF	The link to a 100 Mbps Ethernet network is down.
FDX/COL (Ethernet ports)	Amber	Blinking	The Ethernet port is negotiating in half-duplex mode and collisions are occurring; the more collisions that occur the faster the LED blinks.
		ON	The Ethernet port is negotiating in full-duplex mode.
		OFF	The Ethernet port is negotiating in half-duplex mode and no collisions are occurring.
ACT (GBIC Slots)	Green	On	The port has a successful connection.
		Off	No Ethernet device is connected to this port.
ACT (GBIC Slots)	Green	Blinking	The port is sending or receiving data.
		Off	The port is not sending or receiving data.

3.6 Stacking Scenario Examples

Use Ethernet cables when stacking the switches. See the following figures for example stacking scenarios using the stacking module. The switches must form a closed ring in all scenarios.

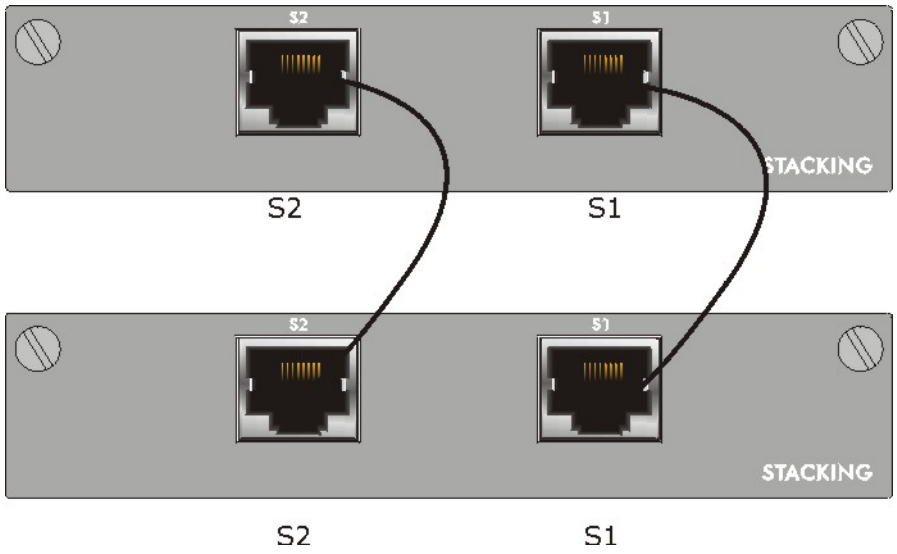


Figure 3-5 Stacking Example 1

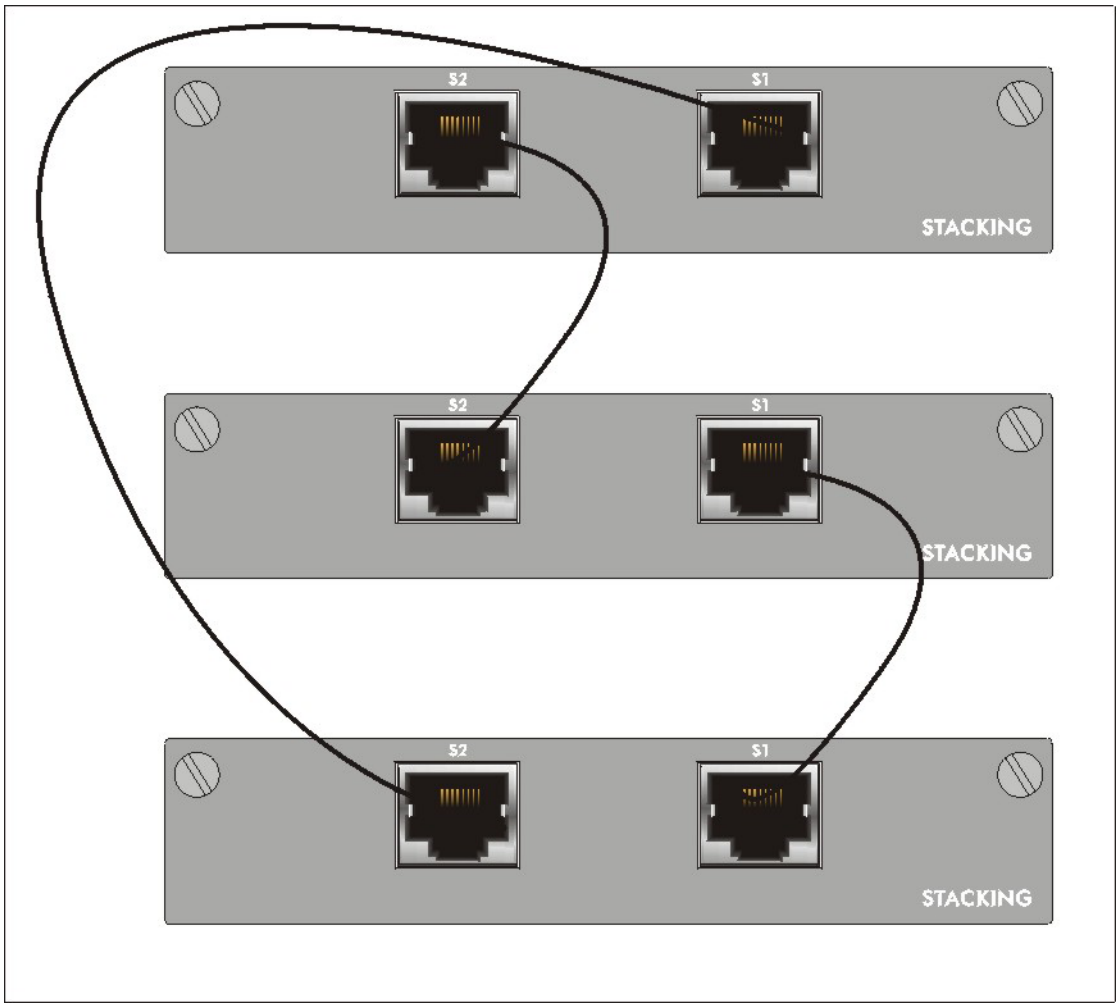


Figure 3-6 Stacking Example 2

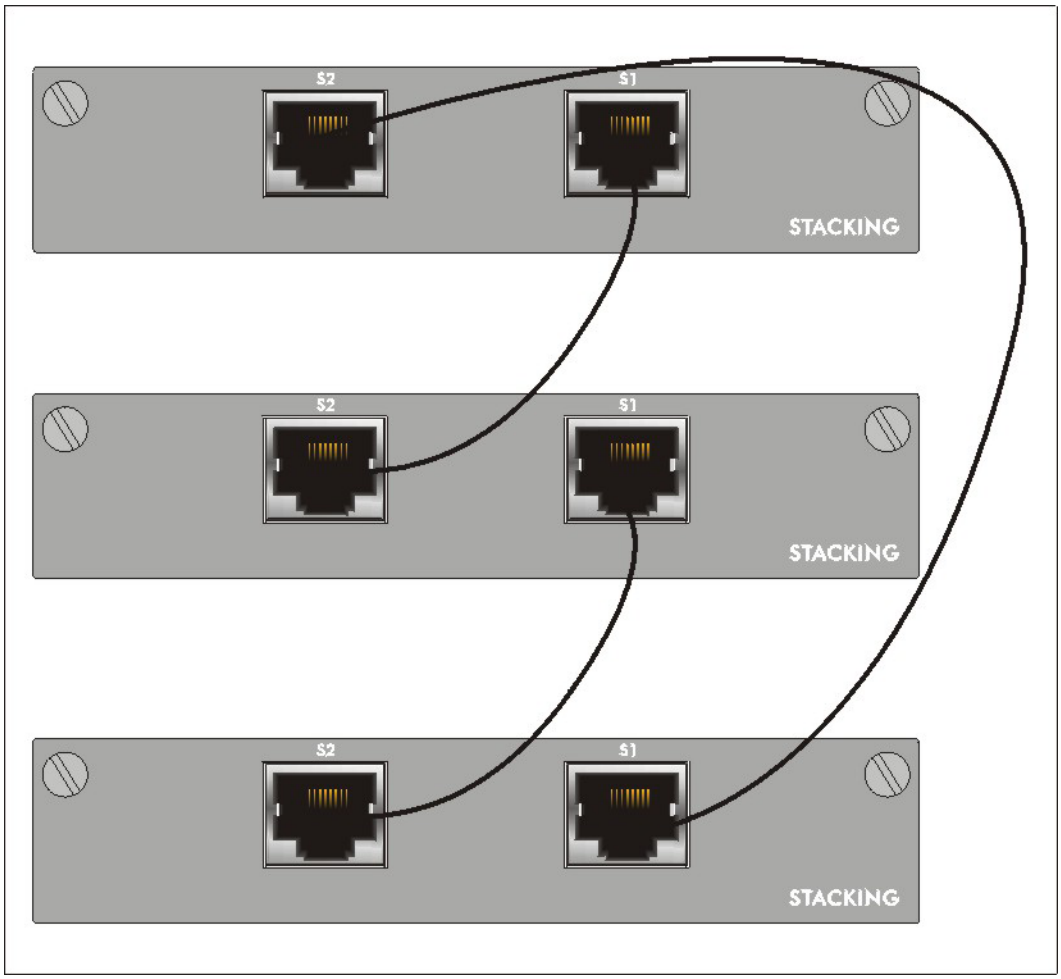


Figure 3-7 Stacking Example 3

See the chapter on CLI commands for information on configuring the stacking modules (as well as other ports) using line commands.

3.7 Uplink Scenario Example

Use Ethernet cables when daisy-chaining/uplinking the switches. See the following figure for an example uplink connection using the stacking module. You must uplink to a Gigabit switch using a cat. 5 Ethernet cable supporting gigabit line rate when uplinking using the stacking module. Uplink scenarios using an uplink module depend on the uplink module you use.

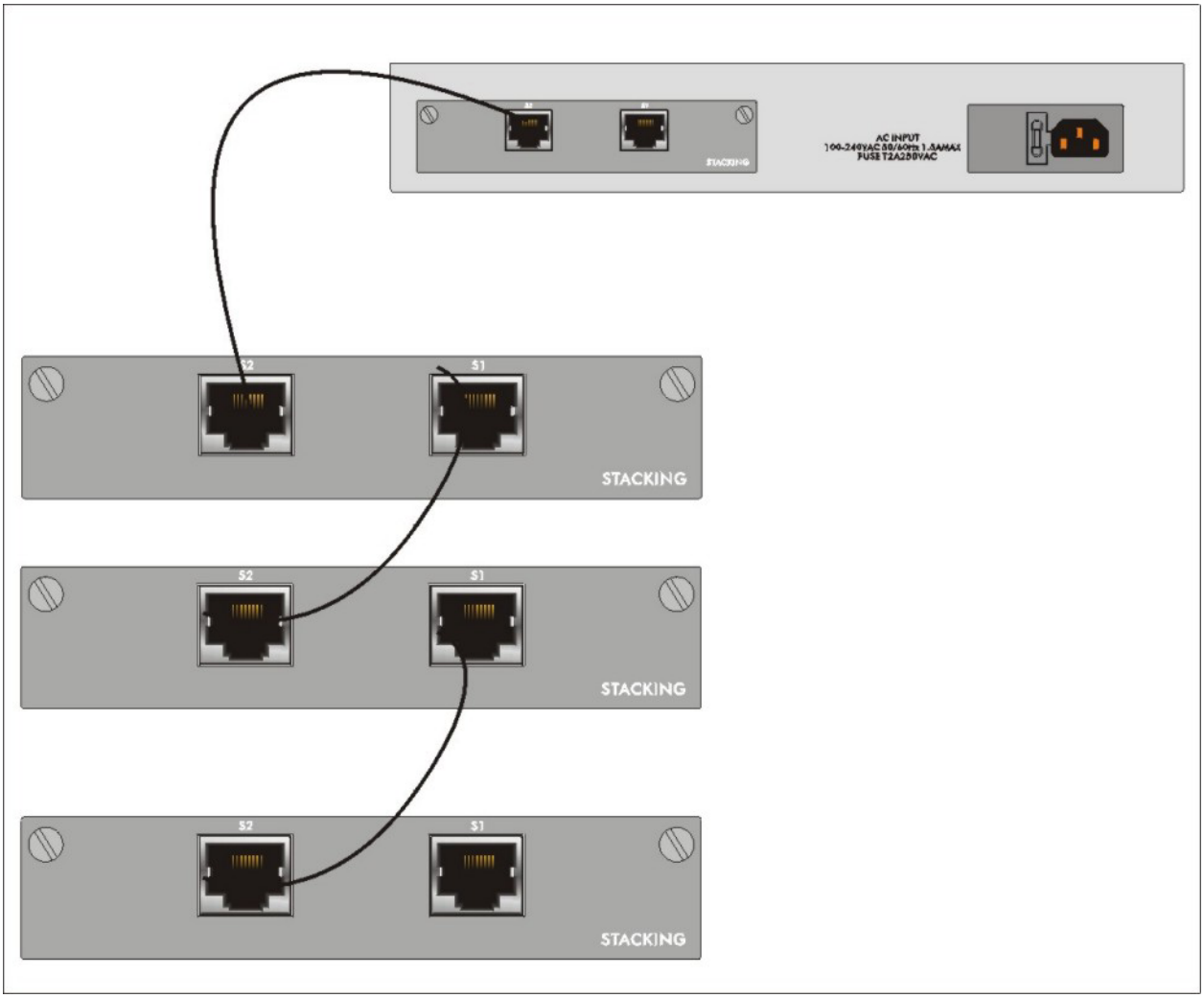


Figure 3-8 Uplink Example

3.8 Accessing the ES-4024

You may use the embedded web configurator or command line interface to configure the ES-4024. If you're using the web configurator, you need Internet Explorer 5.5 and later or Netscape Navigator 6 and later.

You can access the command line interface using a terminal emulation program on a computer connected to the switch console port (see *Section 3.2.1*) or access the switch via an Ethernet port using Telnet.

You can use the "config save" command to save 802.1Q, STP, Cluster and IP configuration changes to non-volatile memory (Flash). These changes are effective after you restart the switch.

However you cannot use "config save" for all other line command configurations. These are saved in volatile memory (DRAM), so are not effective after you restart the switch.

The next part of this guide discusses configuring the ES-4024 using the web configurator.

Part III

Getting Started

This part introduces you to the ES-4024 web configurator, describes the Status and Port Details screens and shows you how to configure the Basic Setting screens.

Chapter 4
Introducing the Web Configurator

This section introduces the configuration and functions of the Web Configurator.

4.1 Introduction

The embedded web configurator allows you to manage the switch from anywhere through a standard browser such as Microsoft Internet Explorer or Netscape Navigator.

Use Internet Explorer 5.5 and later or Netscape Navigator 6 and later versions.

4.2 System Login

Step 1. Start Internet Explorer or Netscape Navigator web browser.

Step 2. Type "http://" and the IP address of the switch (for example, the default is 192.168.1.1) in the Location or Address field. Press **Enter**.

Step 3. The login screen appears. The default username is **admin** and associated default password is **1234**. The date and time display as shown if you have not configured a time server nor manually entered a time and date in the **General Setup** screen.

Figure 4-1 Web Configurator: login

Step 4. Click **OK** to view the first web configurator screen.

4.3 The Status Screen

The **Status** screen is the first screen that displays when you access the web configurator.

The following figure shows the navigating components of a web configurator screen.

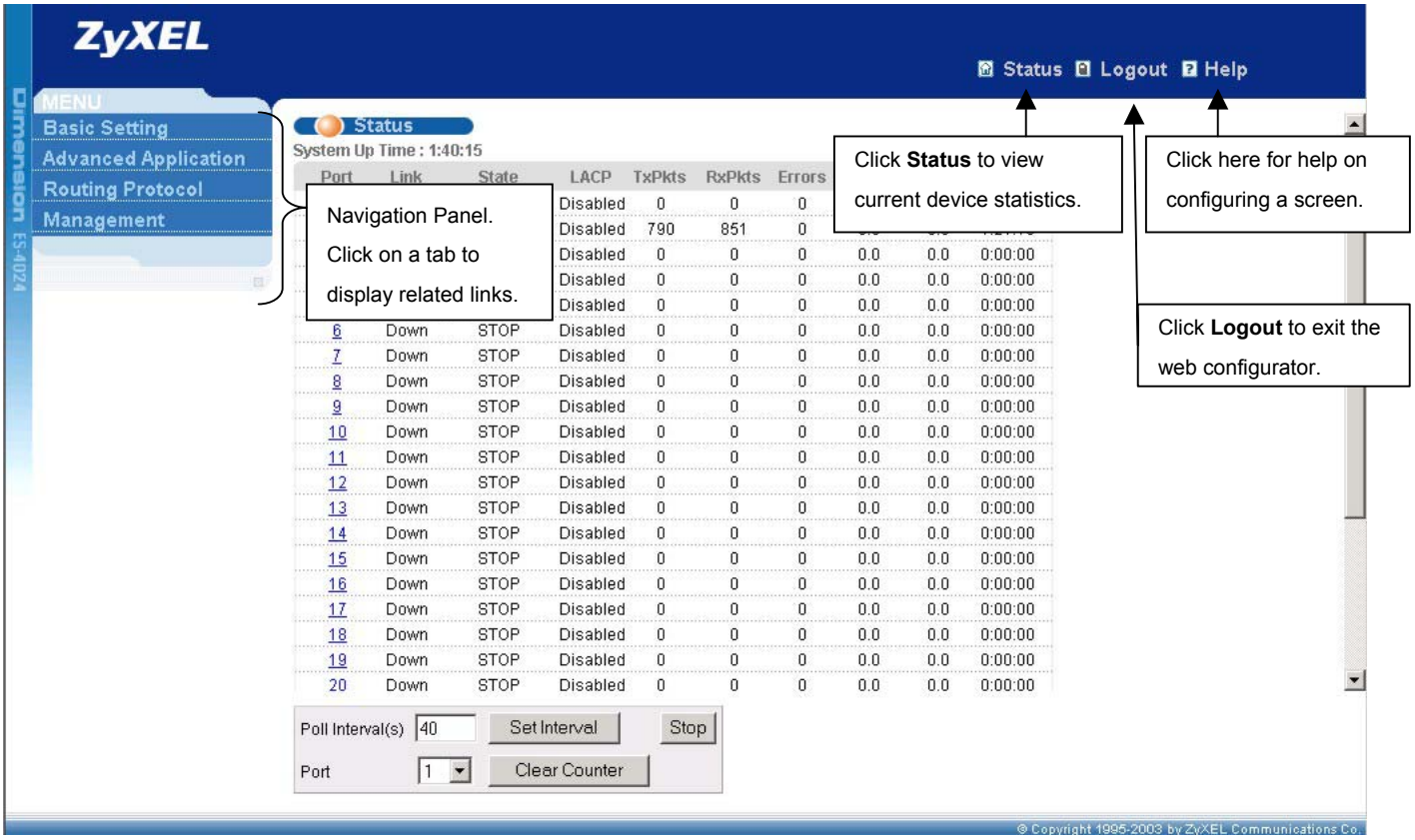
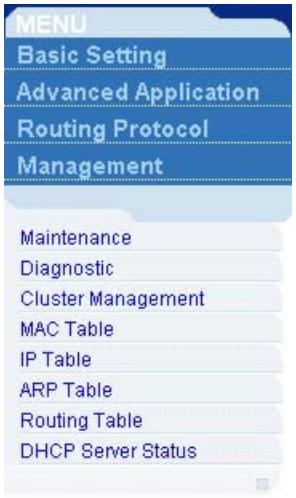


Figure 4-2 Web Configurator Home Screen (Status)

In the navigation panel, click a main link to reveal a list of submenu links.

Table 4-1 Navigation Panel Sub-links Overview

BASIC SETTING	ADVANCED APPLICATION	ROUTING PROTOCOL	MANAGEMENT
			

The following table lists the various web configurator screens within the sub-links.

Table 4-2 Web Configurator Screen Sub-links Details

BASIC SETTING	ADVANCED APPLICATIONS	ROUTING PROTOCOL	MANAGEMENT
System Info	VLAN	Static Routing	Maintenance
General Setup	VLAN Status	RIP	Firmware Upgrade
Switch Setup	VLAN Port Setting	IGMP	Restore Configuration
IP Setup	Static VLAN	DVMRP	Backup Configuration
Port Setup	Static MAC Forwarding	OSPF Status	Load Factory Default
	Filtering	OSPF Configuration	Reboot System
	Spanning Tree Protocol Status	OSPF Interface	Diagnostic
	Spanning Tree Protocol Configuration	OSPF Virtual Link	Cluster Management Status
	Bandwidth Control		Cluster Management Configuration
	Broadcast Storm Control		Filtering Database
	Mirroring		IP Table
	Link Aggregation		ARP Table
	Link Aggregation Protocol Status		Routing Table
	Link Aggregation		DHCP Server Status
	Port Authentication		

Table 4-2 Web Configurator Screen Sub-links Details

BASIC SETTING	ADVANCED APPLICATIONS	ROUTING PROTOCOL	MANAGEMENT
	RADIUS		
	802.1x		
	Port Security		
	DHCP		
	Access Control		
	SNMP		
	Logins		
	Service Access Control		
	Remote Management		
	DiffServ		
	DSCP Setting		
	Marking Rule Setting		
	Queuing Method		
	VRRP Status		
	VRRP Configuration		

The following table describes the links in the navigation panel.

Table 4-3 Navigation Panel Links

LABEL	DESCRIPTION
Basic Settings	
System Info	This link takes you to a screen that displays general system and hardware monitoring information.
General Setup	This link takes you to a screen where you can configure general identification information about the switch.
Switch Setup	This link takes you to a screen where you can set up global switch parameters such as VLAN type, MAC address learning, IGMP snooping, GARP and priority queues.
IP Setup	This link takes you to a screen where you can configure the IP address, subnet mask (necessary for switch management) and DNS (domain name server) and set up to 64 IP routing domains.
Port Setup	This link takes you to screens where you can configure settings for individual switch ports.
Advanced Application	
VLAN	This link takes you to screens where you can configure port-based or 802.1Q VLAN (depending on what you configured in the **Switch Setup** menu).
Static MAC Forwarding	This link takes you to screens where you can configure static MAC addresses for a port. These static MAC addresses do not age out.
Filtering	This link takes you to a screen to set up filtering rules.
Spanning Tree Protocol	This link takes you to screens where you can configure the STP/RSTP to prevent network loops.

Table 4-3 Navigation Panel Links

LABEL	DESCRIPTION
Bandwidth Control	This link takes you to screens where you can cap the maximum bandwidth allowed from specified source(s) to specified destination(s).
Broadcast Storm Control	This link takes you to a screen to set up broadcast filters.
Mirroring	This link takes you to screens where you can copy traffic from one port or ports to another port in order that you can examine the traffic from the first port without interference
Link Aggregation	This link takes you to a screen where you can logically aggregate physical links to form one logical, higher-bandwidth link.
Port Authentication	This link takes you to a screen where you can configure RADIUS (Remote Authentication Dial-In User Service), a protocol for user authentication that allows you to use an external server to validate an unlimited number of users.
Port Security	This link takes you to a screen where you can activate MAC address learning and set the maximum number of MAC addresses to learn on a port.
DHCP	This link takes you to a screen where you can configure the DHCP settings for the network on the ES-4024.
Access Control	This link takes you to screens where you can change the system login password and configure SNMP and remote management.
DiffServ	This link takes you to screens where you can enable DiffServ, configure marking rules and set DSCP-to-IEEE802.1p mappings.
Queuing Method	This link takes you to a screen where you can configure SPQ or WFQ with associated queue weights for each port.
VRRP	This link takes you to screens where you can configure redundant virtual router for your network.
Routing Protocol	
Static Route	This link takes you to screens where you can configure static routes. A static route defines how the ES-4024 should forward traffic by configuring the TCP/IP parameters manually.
RIP	This link takes you to a screen where you can configure the RIP (Routing Information Protocol) direction and versions.
IGMP	This link takes you to a screen where you can configure the IGMP settings.
DVMRP	This link takes you to a screen where you can configure the DVMRP (Distance Vector Multicast Routing Protocol) settings.
OSPF	This link takes you to screens where you can view the OSPF status and configure OSPF settings.
Advanced Management	
Maintenance	This link takes you to screens where you can perform firmware and configuration file maintenance as well as reboot the system.
Diagnostic	This link takes you to screens where you can view system logs and test port(s).
Cluster Management	This link takes you to a screen where you can configure clustering management and view its status.
MAC Table	This link takes you to a screen where you can view the MAC addresses (and types) of devices attached to what ports and VLAN IDs.

Table 4-3 Navigation Panel Links

LABEL	DESCRIPTION
IP Table	This link takes you to a screen where you can view the IP addresses (and types) of devices attached to what ports and VLAN IDs.
ARP Table	This link takes you to a screen where you can view the MAC addresses – IP address resolution table.
Routing Table	This link takes you to a screen where you can view the routing table in the ES.
DHCP Server Status	This link takes you to screens where you can view the general and detail DHCP server status.

4.3.1 Change Your Password

After you log in for the first time, it is recommended you change the default administrator password. Click **Advanced Application**, **Access Control** and then **Logins** to display the next screen.

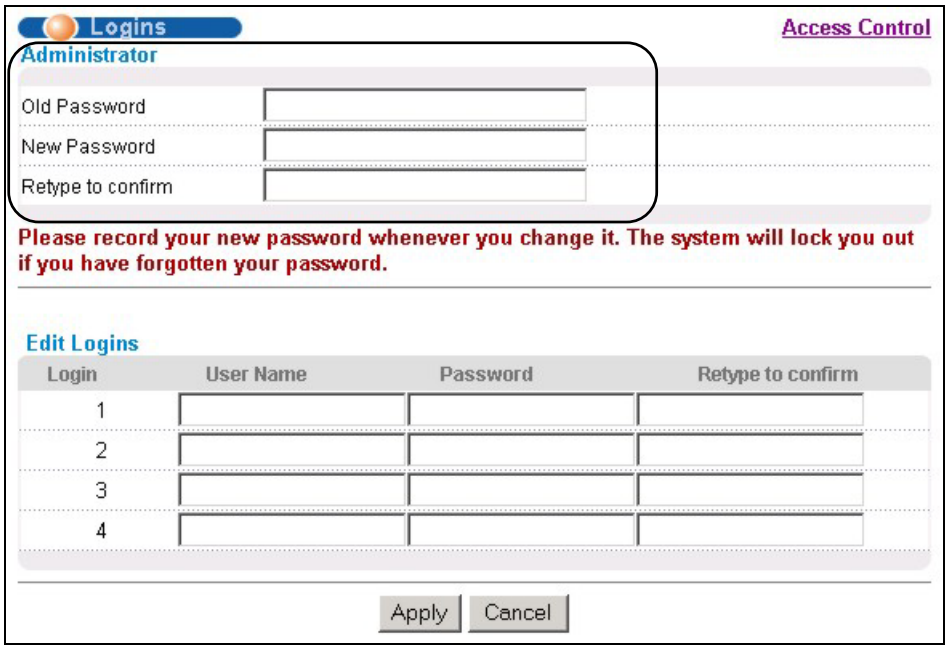


Figure 4-3 Change Administrator Login Password

4.4 Switch Lockout

You are locked out from managing the switch if another administrator is currently logged in. You must wait until he/she has logged out before you can log in.

Moreover, you could lock yourself (and all others) out from the switch by:

1. Deleting the management VLAN (default is VLAN 1).
2. Deleting all IP routing domains.

3. Deleting all port-based VLANs with the CPU port as a member. The "CPU port" is the management port of the switch.
4. Filtering all traffic to the CPU port.
5. Disabling all ports.
6. Assigning minimum bandwidth to the CPU port. If you limit bandwidth to the CPU port, you may find that the switch performs sluggishly or not at all.

Be careful not to lock yourself and others out of the switch.

4.5 Resetting the Switch

If you lock yourself (and others) from the switch or forget the ES-4024 password, you will need to reload the factory-default configuration file.

Uploading the factory-default configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all previous configurations and the speed of the console port will be reset to the default of 9600bps with 8 data bit, no parity, one stop bit and flow control set to none. The password will also be reset to "1234" and the IP address to 192.168.1.1.

To upload the configuration file, do the following:

Step 1. Connect to the console port using a computer with terminal emulation software. See the chapter on hardware connections for details.

Step 2. Disconnect and reconnect the switch's power to begin a session. When you reconnect the switch's power, you will see the initial screen.

Step 3. When you see the message "`Press any key to enter Debug Mode within 3 seconds`" press any key to enter debug mode.

Step 4. Type `atlc` after the "`Enter Debug Mode`" message.

Step 5. Wait for the "`Starting XMODEM upload`" message before activating XMODEM upload on your terminal.

Step 6. After a configuration file upload, type `atgo` to restart the switch.

```
Bootbase Version: V1.0 | 04/25/2003 10:01:06
RAM: Size = 32768 Kbytes
FLASH: Intel 32M

ZyNOS Version: V3.50(DU.0)b6 | 07/11/2003 18:00:29

Press any key to enter debug mode within 3 seconds.
.....................
Enter Debug Mode
ES-4024> atlc

Starting XMODEM upload (CRC mode)....
CCCCCCCCCCCCCCC
Total  262144 bytes received.

Erasing..
.............................................................
OK
ES-4024> atgo
```

Figure 4-4 Resetting the Switch: Via Console Port

The switch is now reinitialized with a default configuration file including the default password of "1234".

4.5.1 Logging Out of the Web Configurator

Click **Logout** in a screen to exit the web configurator. You have to log in with your password again after you log out. This is recommended after you finish a management session both for security reasons and so as you don't lock out other switch administrators.

Figure 4-5 Web Configurator: Logout Screen

4.5.2 Help

The web configurator's online help has descriptions of individual screens and some supplementary information.

Click the **Help** link from a web configurator screen to view an online help description of that screen.

Chapter 5
System Status and Port Statistics

This chapter describes the system status (web configurator home page) and port details screens.

5.1 About System Statistics and Information

The home screen of the web configurator displays a port statistical summary with links to each port showing statistical details.

5.2 Port Status Summary

To view the port statistics, click **Status** in all web configurator screens to display the **Status** screen as shown next.

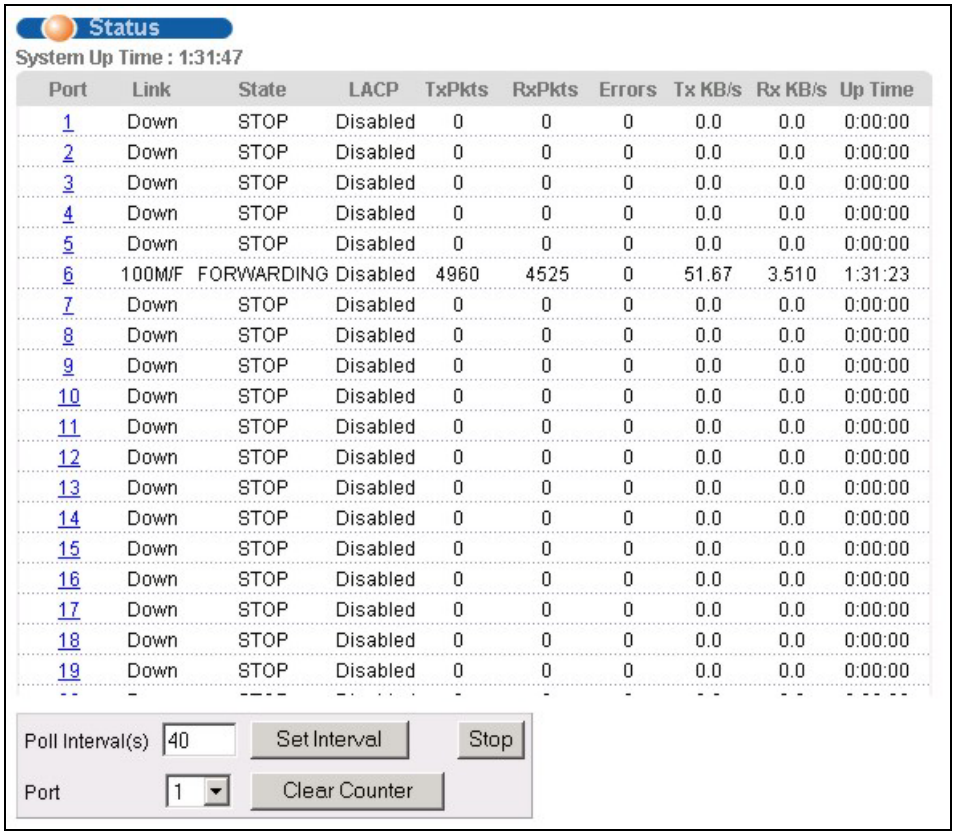


Figure 5-1 Status

The following table describes the labels in this screen.

Table 5-1 Status

LABEL	DESCRIPTION
System up Time	This field shows how long the system has been running since the last time it was started.
Port	This identifies the Ethernet port. Click a port number to display the **Port Details** screen (refer to *Section 5.2.1*).
Link	This field displays the speed (either **10M** for 10Mbps, **100M** for 100Mbps or another value depending on the uplink module being used) and the duplex (**F** for full duplex or **H** for half).
State	This field displays the STP (Spanning Tree Protocol) state of the port. See the chapter on STP for details on STP states.
LACP	This fields displays whether LACP (Link Aggregation Control Protocol) has been enabled on the port.
TxPkts	This field shows the number of transmitted frames on this port.
RxPkts	This field shows the number of received frames on this port.
Errors	This field shows the number of received errors on this port.
Tx KB/s	This field shows the number of kilobytes per second transmitted on this port.
Rx KB/s	This field shows the number of kilobytes per second received on this port.
Up Time	This field shows the total amount of time in hours, minutes and seconds the port has been up.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt system statistic polling.
Clear Counter	Select a port from the **Port** drop-down list box and then click **Clear Counter** to erase the recorded statistical information for that port.

5.2.1 Port Details

Click a number in the **Port** column in the **Status** screen to display individual port statistics. Use this screen to check status and detailed performance data about an individual port on the switch.

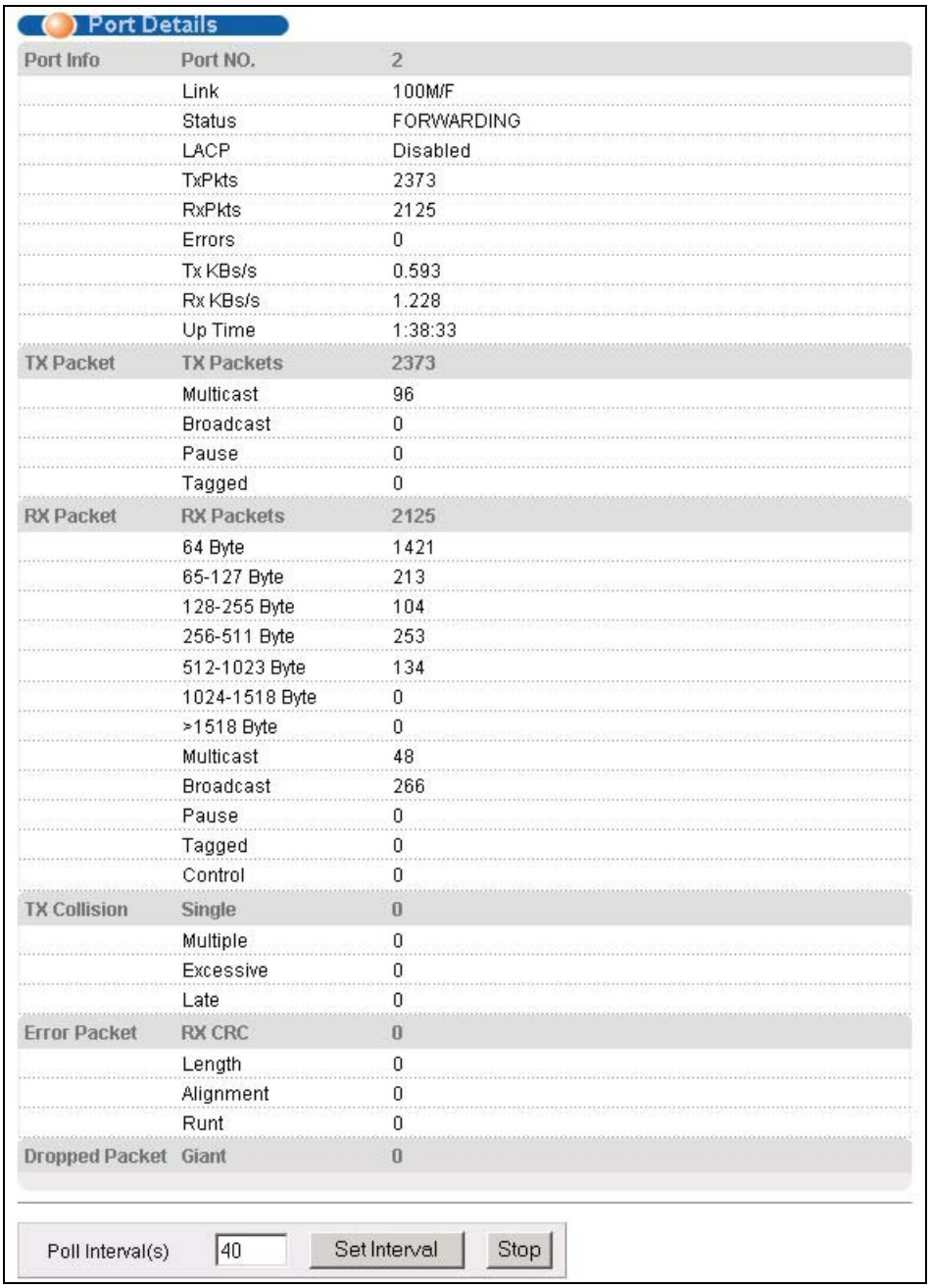


Figure 5-2 Status: Port Details

The following table describes the labels in this screen.

Table 5-2 Status: Port Details

LABEL	DESCRIPTION
Port Info	
Link	This field shows whether the Ethernet connection is down, and the speed/duplex mode.

Table 5-2 Status: Port Details

LABEL	DESCRIPTION
Status	This field shows the training state of the ports. The states are **FORWARDING** (forwarding), which means the link is functioning normally or **STOP** (the port is stopped to break a loop or duplicate path).
LACP	This field shows if LACP is enabled on this port or not.
TxPkts	This field shows the number of transmitted frames on this port
RxPkts	This field shows the number of received frames on this port
Errors	This field shows the number of received errors on this port.
Tx KB/s	This field shows the number kilobytes per second transmitted on this port.
Rx KB/s	This field shows the number of kilobytes per second received on this port.
Up Time	This field shows the total amount of time the connection has been up.
Tx Packet The following fields display detailed information about packets transmitted.	
TX	This field shows the number of good packets (unicast, multicast and broadcast) transmitted.
Multicast	This field shows the number of good multicast packets transmitted.
Broadcast	This field shows the number of good broadcast packets transmitted.
Pause	This field shows the number of 802.3x Pause packets transmitted.
Tagged	This field shows the number of packets with VLAN tags transmitted.
Rx Packet The following fields display detailed information about packets received.	
RX	This field shows the number of good packets (unicast, multicast and broadcast) received.
64	This field shows the number of packets (including bad packets) received that were 64 octets in length.
65-127	This field shows the number of packets (including bad packets) received that were between 65 and 127 octets in length.
128-255	This field shows the number of packets (including bad packets) received that were between 128 and 255 octets in length.
256-511	This field shows the number of packets (including bad packets) received that were between 256 and 511 octets in length.
512-1023	This field shows the number of packets (including bad packets) received that were between 512 and 1023 octets in length.
1024-1518	This field shows the number of packets (including bad packets) received that were between 1024 and 1518 octets in length.

Table 5-2 Status: Port Details

LABEL	DESCRIPTION
>1518	This field shows the number of packets (including bad packets) transmitted that were greater than 1518 octets in length.
Multicast	This field shows the number of good multicast packets received.
Broadcast	This field shows the number of good broadcast packets received.
Pause	This field shows the number of 802.3x Pause packets received.
Tagged	This field shows the number of packets with VLAN tags received.
Control	This field shows the number of control packets received (including those with CRC error) but it does not include the 802.3x Pause packets.
TX Collision The following fields display information on collisions while transmitting.	
Single	This is a count of successfully transmitted packets for which transmission is inhibited by exactly one collision.
Multiple	This is a count of successfully transmitted packets for which transmission was inhibited by more than one collision.
Excessive	This is a count of packets for which transmission failed due to excessive collisions. Excessive collision is defined as the number of maximum collisions before the retransmission count is reset.
Late	This is the number of times a late collision is detected, that is, after 512 bits of the packets have already been transmitted.
Error Packet	The following fields display detailed information about packets received that were in error.
RX CRC	This field shows the number of packets received with CRC (Cyclic Redundant Check) error(s).
Length	This field shows the number of packets received with a length that was out of range.
Alignment	This field shows the number of packets received of proper size but with CRC error(s) and a non-integral number of octets.
Runt	This field shows the number of packets received that were too short (shorter than 64 octets), including the ones with CRC errors.
Dropped Packet	The following filed indicates why packets were dropped.
Giant	This field shows the number of packets dropped because they were bigger than the maximum frame size.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to stop port statistic polling.

Chapter 6
Basic Setting

*This chapter describes how to configure the **System Info, General Setup**, **Switch Setup**, **IP Setup** and **Port Setup** screens.*

6.1 Introducing The Basic Setting Screens

The **System Info** screen displays general switch information (such as firmware version number) and hardware polling information (such as fan speeds). The **General Setup** screen allows you to configure general switch identification information. The **General Setup** screen also allows you to set the system time manually or get the current time and date from an external server when you turn on your switch. The real time is then displayed in the switch logs. The **Switch Setup** screen allows you to set up and configure global switch features. The **IP Setup** screen allows you to configure a switch IP address in each routing domain, subnet mask(s) and DNS (domain name server) for management purposes.

6.2 System Information

In the navigation panel, click **Basic Setting** and **System Info** to display the screen as shown. You can check the firmware version number and monitor the switch temperature, fan speeds and voltage in this screen.

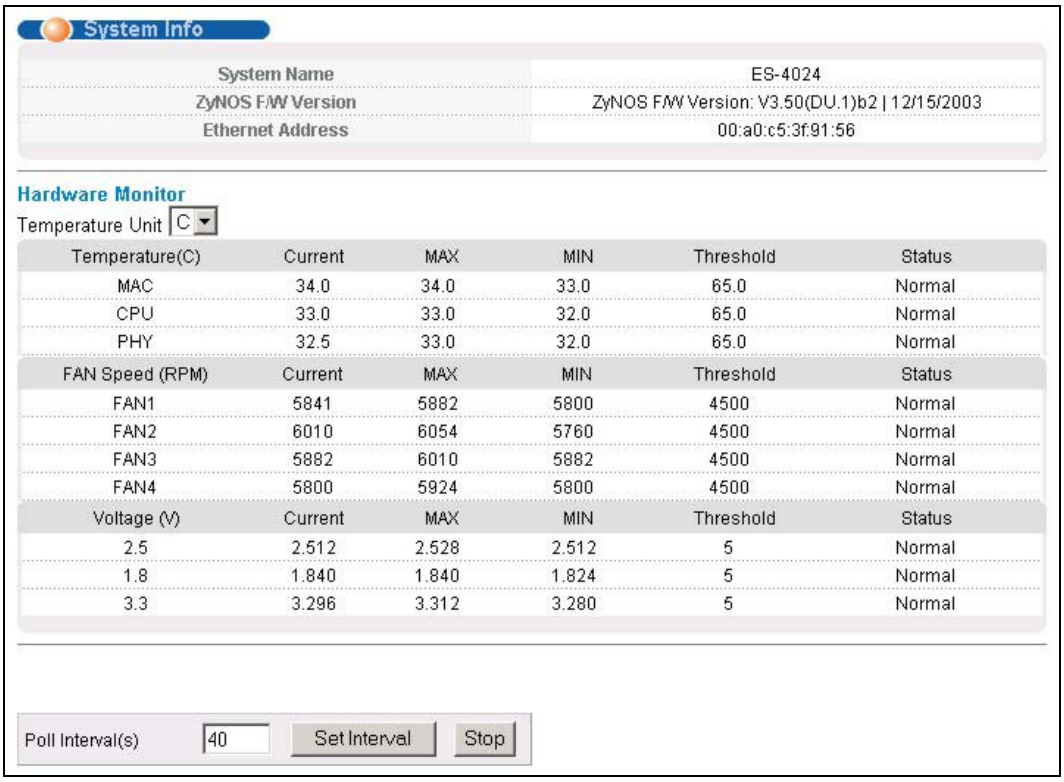


Figure 6-1 Basic Setting: System Info

The following table describes the labels in this screen.

Table 6-1 Basic Setting: System Info

LABEL	DESCRIPTION
System Name	This field displays the switch 's model name.
ZyNOS F/W Version	This field displays the version number of the switch 's current firmware including the date created.
Ethernet Address	This field refers to the Ethernet MAC (Media Access Control) address of the switch.
Hardware Monitor	
Temperature Unit	The switch has temperature sensors that are capable of detecting and reporting if the temperature rises above the threshold. You may choose the temperature unit (Centigrade or Fahrenheit) in this field.
Temperature	**MAC**, **CPU** and **PHY** refer to the location of the temperature sensors on the switch printed circuit board.
Current	This shows the current temperature in degrees centigrade at this sensor.
MAX	This field displays the maximum temperature measured at this sensor.
MIN	This field displays the minimum temperature measured at this sensor.
Threshold	This field displays the upper temperature limit at this sensor.
Status	This field displays **Normal** for temperatures below the threshold and **Error** for those above.
Fan Speed (RPM)	A properly functioning fan is an essential component (along with a sufficiently ventilated, cool operating environment) in order for the device to stay within the temperature threshold. Each fan has a sensor that is capable of detecting and reporting if the fan speed falls below the threshold shown.
Current	This field displays this fan's current speed in Revolutions Per Minute (RPM).
MAX	This field displays this fan's maximum speed measured in Revolutions Per Minute (RPM).
MIN	This field displays this fan's minimum speed measured in Revolutions Per Minute (RPM). "<41" is displayed for speeds too small to measure (under 2000 RPM).
Threshold	This field displays the minimum speed at which a normal fan should work.
Status	**Normal** indicates that this fan is functioning above the minimum speed. **Error** indicates that this fan is functioning below the minimum speed.
Voltage(V)	The power supply for each voltage has a sensor that is capable of detecting and reporting if the voltage falls out of the tolerance range.
Current	This is the current voltage reading.
MAX	This field displays the maximum voltage measured at this point.
MIN	This field displays the minimum voltage measured at this point.

Table 6-1 Basic Setting: System Info

LABEL	DESCRIPTION
Threshold	This field displays the minimum voltage at which the switch should work.
Status	**Normal** indicates that the voltage is within an acceptable operating range at this point; otherwise **Error** is displayed.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt statistic polling.

6.3 General Setup

Click **Basic Setting** and **General Setup** in the navigation panel to display the screen as shown.

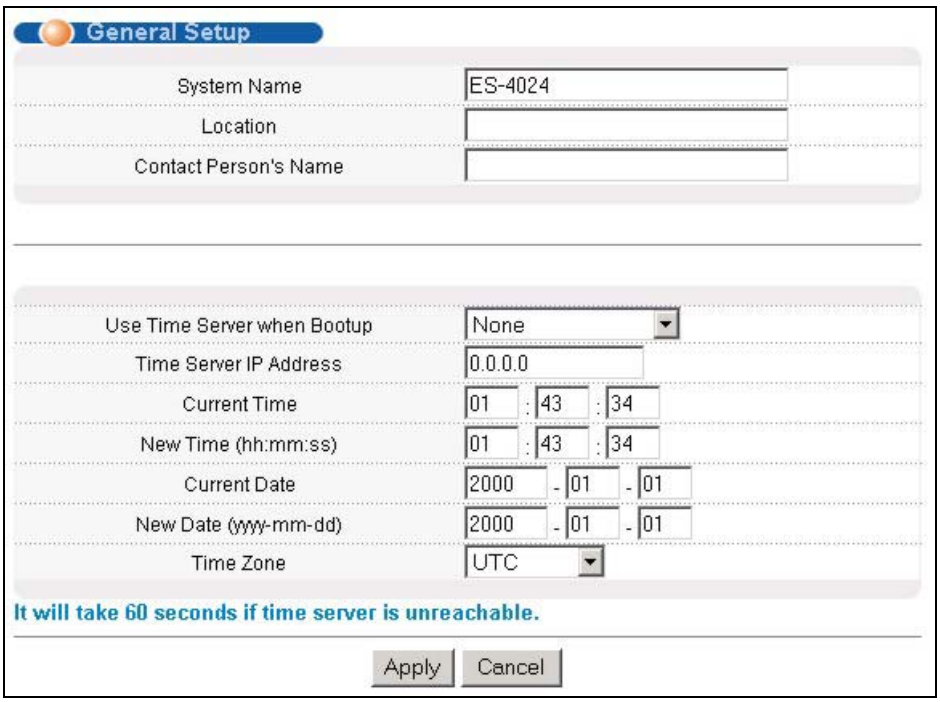


Figure 6-2 Basic Setting: General Setup

The following table describes the labels in this screen.

Table 6-2 Basic Setting: General Setup

LABEL	DESCRIPTION
System Name	Choose a descriptive name for identification purposes. This name consists of up to 32 printable characters; spaces are not allowed.
Location	Enter the geographic location (up to 30 characters) of your switch.

Table 6-2 Basic Setting: General Setup

LABEL	DESCRIPTION
Contact Person's Name	Enter the name (up to 30 characters) of the person in charge of this switch.
Use Time Server when Bootup	Enter the time service protocol that a timeserver sends when you turn on the switch. Not all timeservers support all protocols, so you may have to use trial and error to find a protocol that works. The main differences between them are the time format. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **Time (RFC-868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. **NTP (RFC-1305)** is similar to Time (RFC-868). **None** is the default value. Enter the time manually. Each time you turn on the switch, the time and date will be reset to 2000-1-1 0:0.
Time Server IP Address	Enter the IP address (or URL if you configure a domain name server in the **IP Setup** screen) of your timeserver. The switch searches for the timeserver for up to 60 seconds. If you select a timeserver that is unreachable, then this screen will appear locked for 60 seconds. Please wait.
Current Time	This field displays the time you open this menu (or refresh the menu).
New Time (hh:min:ss)	Enter the new time in hour, minute and second format. The new time then appears in the **Current Time** field after you click **Apply**.
Current Date	This field displays the date you open this menu.
New Date (yyyy-mm-dd)	Enter the new date in year, month and day format. The new date then appears in the **Current Date** field after you click **Apply**.
Time Zone	Select the time difference between UTC (Universal Time Coordinated, formerly known as GMT, Greenwich Mean Time) and your time zone from the drop-down list box.
Apply	Click **Apply** to save the settings.
Cancel	Click **Cancel** to reset the fields to your previous configuration.

6.4 Introduction to VLANs

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

In MTU (Multi-Tenant Unit) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user in the same building.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

Note that VLAN is unidirectional; it only governs outgoing traffic.

See the *VLAN* chapter for information on port-based and 802.1Q tagged VLANs.

6.5 IGMP Snooping

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. Refer to RFC 2236 for information IGMP version 2 and RFC 1112 for IGMP version 1.

A layer-2 switch can passively snoop on IGMP Query, Report and Leave (IGMP version 2) packets transferred between IP multicast routers/switches and IP multicast hosts to learn the IP multicast group membership. It checks IGMP packets passing through it, picks out the group registration information, and configures multicasting accordingly.

Without IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic, that is, it is forwarded to all ports. With IGMP snooping, group multicast traffic is only forwarded to ports that are members of that group. IGMP Snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your switch.

6.6 Switch Setup Screen

Click **Basic Setting** and then **Switch Setup** in the navigation panel to display the screen as shown. The VLAN setup screens change depending on whether you choose **802.1Q** or **Port Based** in the **VLAN Type** field in this screen. Refer to the chapter on VLAN.

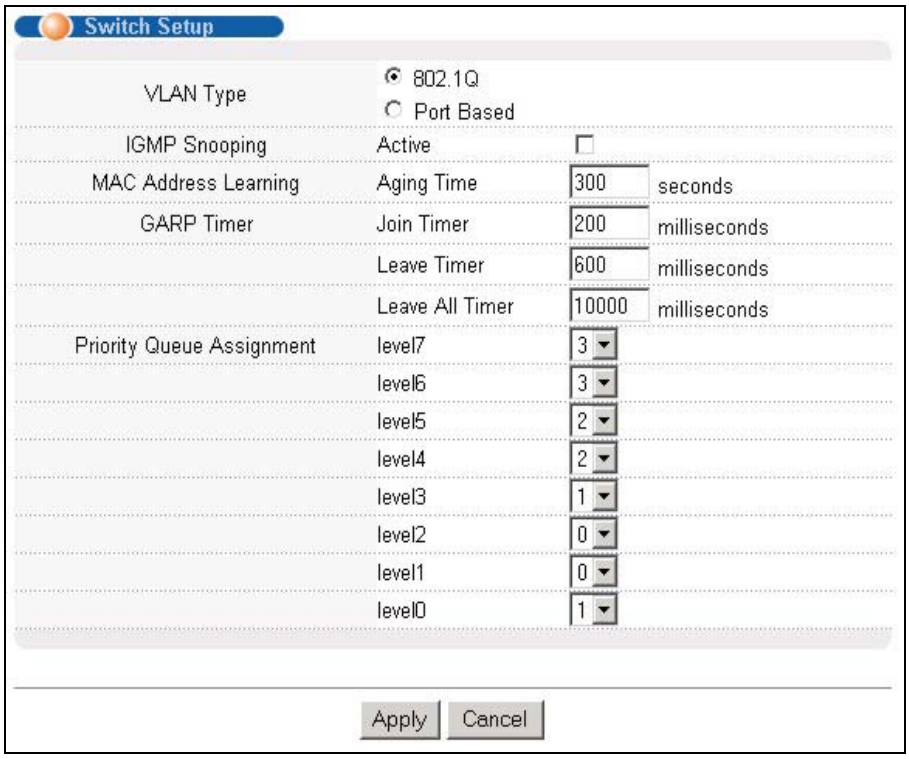


Figure 6-3 Basic Setting: Switch Setup

The following table describes the labels in this screen.

Table 6-3 Basic Setting: Switch Setup

LABEL	DESCRIPTION	EXAMPLE
VLAN Type	Choose **802.1Q** or **Port Based**. The **VLAN Setup** screen changes depending on whether you choose **802.1Q** VLAN type or **Port Based** VLAN type in this screen. See *Section 6.4* and the chapter on VLAN for more information.	802.1Q
IGMP Snooping	Select the **Active** checkbox to enable IGMP snooping have group multicast traffic only forwarded to ports that are members significantly reducing multicast traffic passing through your switch. See *Section 6.5* for more information on IGMP snooping. **You *cannot* enable both IGMP snooping and IGMP at the same time. Refer to the section on IGMP for more information.**	
MAC Address Learning	MAC address learning reduces outgoing traffic broadcasts. For MAC address learning to occur on a port, the port must be active.	
Aging Time	Enter a time from 10 to 3000 seconds. This is how long all dynamically learned MAC addresses remain in the MAC address table before they age out (and must be relearned).	300
GARP Timer: Switches join VLANs by making a declaration. A declaration is made by issuing a **Join** message using GARP. Declarations are withdrawn by issuing a **Leave** message. A **Leave All** message terminates all registrations. GARP timers set declaration timeout values. See the chapter on VLAN setup for more background information.		
Join Timer	Join Timer sets the duration of the Join Period timer for GVRP in milliseconds. Each port has a Join Period timer. The allowed Join Time range is between 100 and 65535 milliseconds; the default is 200 milliseconds. See the chapter on VLAN setup for more background information.	200 milliseconds (default)
Leave Timer	Leave Timer sets the duration of the Leave Period timer for GVRP in milliseconds. Each port has a single Leave Period timer. Leave Time must be two times larger than Join Timer; the default is 600 milliseconds.	600 milliseconds (default)
Leave All Timer	Leave All Timer sets the duration of the Leave All Period timer for GVRP in milliseconds. Each port has a single Leave All Period timer. Leave All Timer must be larger than Leave Timer; the default is 1000 milliseconds.	1000 milliseconds (default)
Priority Queue Assignment IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Frames without an explicit priority tag are given the default priority of the ingress port. Use the next two fields to configure the priority level-to-physical queue mapping. The switch has 4 physical queues that you can map to the 8 priority levels. On the switch, traffic assigned to higher index queues gets through faster while traffic in lower index queues is dropped if the network is congested.		
Priority Level (The following descriptions are based on the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).		
Level 7	Typically used for network control traffic such as router configuration messages.	
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).	

Table 6-3 Basic Setting: Switch Setup

LABEL	DESCRIPTION	EXAMPLE
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.	
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.	
Level 3	Typically used for “excellent effort” or better than best effort and would include important business traffic that can tolerate some delay.	
Level 2	This is for “spare bandwidth”.	
Level 1	This is typically used for non-critical “background” traffic such as bulk transfers that are allowed but that should not affect other applications and users.	
Level 0	Typically used for best-effort traffic.	
Apply	Click **Apply** to save the settings.	
Cancel	Click **Cancel** to reset the fields to your previous configuration.	

6.7 IP Setup

Use the **IP Setup** screen to configure the default gateway device, the default domain name server and add IP domains.

6.7.1 Default Gateway and Domain Name Server

To set the default gateway device and the domain name server on the switch, click **Basic Setting** and **IP Setup** in the navigation panel to display the screen as shown. The default gateway specifies the IP address of the default gateway (next hop) for outgoing traffic.

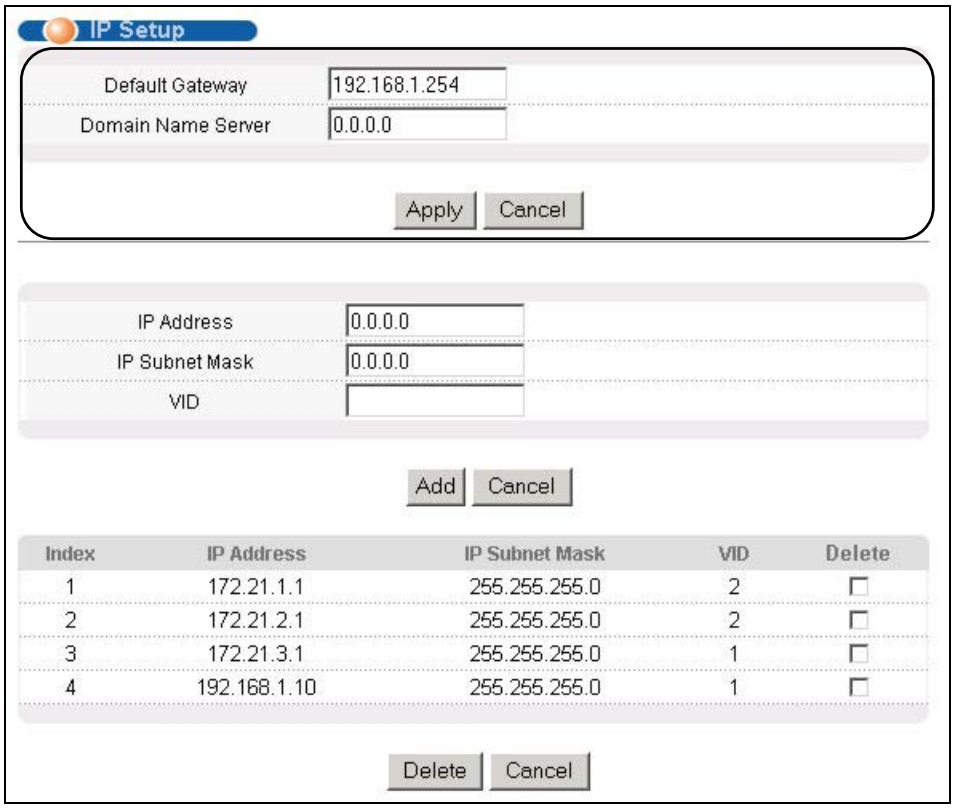


Figure 6-4 Basic Setting: IP Setup: Default Gateway and Domain Name Server

The following table describes the related labels in the **IP Setup** screen.

Table 6-4 Basic Setting: IP Setup: Default Gateway and Domain Name Server

LABEL	DESCRIPTION
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
Domain Name Server	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. Enter a domain name server IP address in order to be able to use a domain name instead of an IP address.
Apply	Click **Apply** to save the settings.
Cancel	Click **Cancel** to reset the fields to your previous configuration.

6.7.2 Configure IP Interfaces

The switch needs an IP address for it to be managed over the network. The factory default IP address is 192.168.1.1. The subnet mask specifies the network number portion of an IP address. The factory default subnet mask is 255.255.255.0.

The ES, as a layer 3 device, associates an IP address to a virtual routing interface (or VLAN). When routing between VLANs, IP addresses are associated with the VLANs and not to any physical interfaces. Since each IP

address on the ES must be in a separate subnet, the configured IP address is also known as IP routing domain. In addition, this allows IP routing between subnets without additional routers.

You can configure multiple routing domains (up to 64) on the same VLAN as long as the IP address ranges for the domains do not overlap. To change the IP address of the switch in a routing domain, simply add a new routing domain entry with a different IP address in the same subnet.

Set the related fields in the **IP Setup** screen.

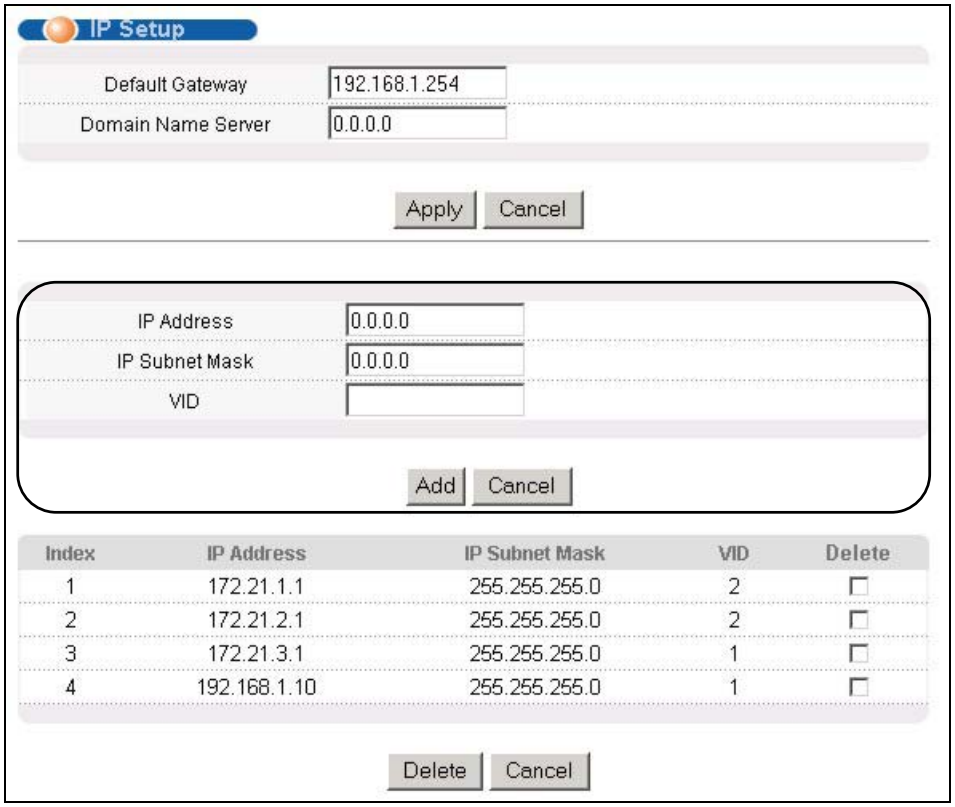


Figure 6-5 IP Setup: Configure IP Routing Domains

The following table describes the related labels in the **IP Setup** screen.

Table 6-5 IP Setup: Configure IP Routing Domains

LABEL	DESCRIPTION
IP Address	Enter the IP address of your switch in dotted decimal notation for example 192.168.1.1. This is the IP address of the switch in an IP routing domain.
IP Subnet Mask	Enter the IP subnet mask of an IP routing domain in dotted decimal notation. For example, 255.255.255.0.
VID	Enter the VLAN identification number to which an IP routing domain belongs.
Add	Click **Add** to save the new rule to the switch. It then displays in the summary table at the bottom of the screen.
Cancel	Click **Cancel** to reset the fields to your previous configuration.

6.7.3 View Switch IP Settings

To view the switch IP settings, scroll down to the table in the **IP Setup** screen.

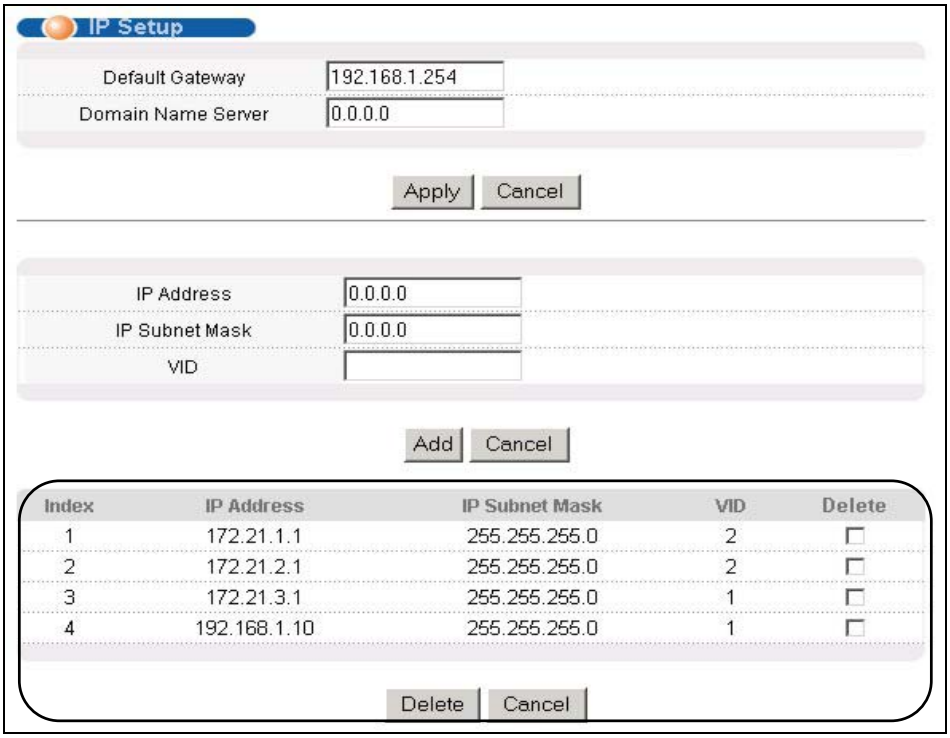


Figure 6-6 IP Setup: View Settings

The following table describes the related labels in the information table.

Table 6-6 IP Setup: View Settings

LABEL	DESCRIPTION
Index	This field displays the index number of an entry.
IP Address	This field displays IP address of the switch in the IP domain.
Subnet Mask	This field displays the subnet mask of the switch in the IP domain.
VID	This field displays the VLAN identification number of the IP domain on the switch.
Delete	Click **Delete** to remove the selected entry from the summary table.
	Deleting all IP domains locks you out from the switch.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

6.8 Port Setup

Click **Basic Setting** and then **Port Setup** in the navigation panel to enter the port configuration screen. You may configure any of the 28 Ethernet ports (ports S1 and S2 are the gigabit ports on the GBIC modules).

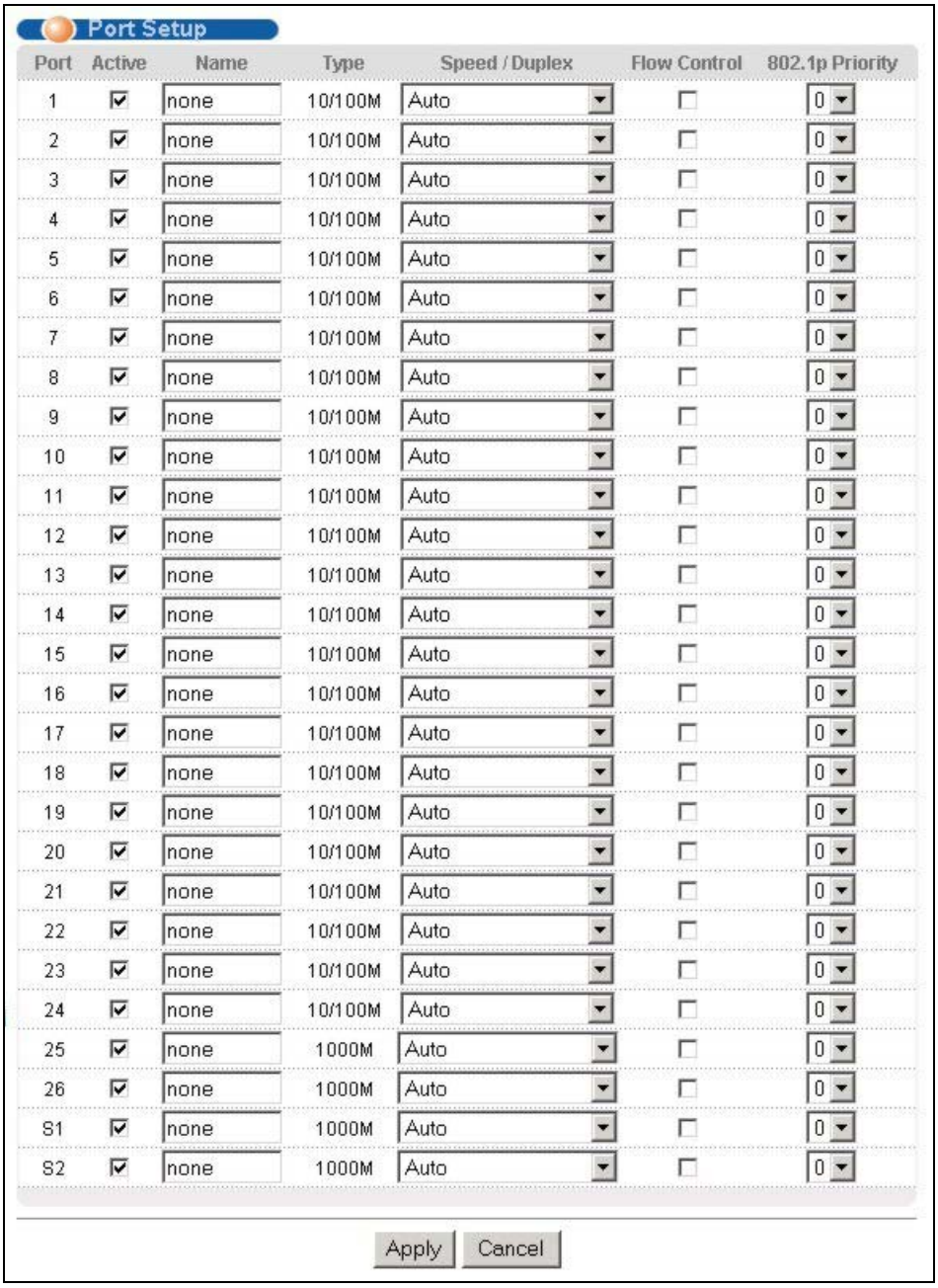


Figure 6-7 Basic Setting: Port Setup

The following table describes the labels in this screen.

Table 6-7 Basic Setting: Port Setup

LABEL	DESCRIPTION
Port	This is the port index number.
Active	Select this check box to enable a port. The factory default for all ports is enabled. A port must be enabled for data transmission to occur.
Name	Enter a descriptive name that identifies this port.

Table 6-7 Basic Setting: Port Setup

LABEL	DESCRIPTION
Type	This field displays **10/100M** for an Ethernet/Fast Ethernet connection and **1000M** for the uplink ports.
Speed/Duplex	Select the speed and the duplex mode of the Ethernet connection on this port. Choices are **Auto**, **10M/Half Duplex**, **10M/Full Duplex**, **100M/Half Duplex**, **100M/Full Duplex** and **1000M/Full Duplex** (for gigabit ports only). Selecting **Auto** (auto-negotiation) allows one Ethernet port to negotiate with a peer automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, an Ethernet port on the switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer Ethernet port does not support auto-negotiation or turns off this feature, the switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the switch's auto-negotiation is turned off, an Ethernet port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer Ethernet port are the same in order to connect.
Flow Control	A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. **Flow Control** is used to regulate transmission of signals to match the bandwidth of the receiving port. The ES-4024 uses IEEE802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later. Select **Flow Control** to enable it.
802.1P Priority	This priority value is added to incoming frames without a (802.1p) priority queue tag. See **Priority Queue Assignment** in *Table 6-3* for more information.
Apply	Click **Apply** to save the settings.
Cancel	Click **Cancel** to reset the fields to your previous configuration.

Part IV

Advanced Application

This part shows you how to configure the Advanced Application screens.

Chapter 7 VLAN

*The type of screen you see here depends on the **VLAN Type** you selected in the **Switch Setup** screen. This chapter shows you how to configure 802.1Q tagged and port-based VLANs. See the General, Switch and IP Setup sections for more information.*

7.1 Introduction to IEEE 802.1Q Tagged VLAN

Tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier, residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information, starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 (212) VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094

TPID 2 Bytes	User Priority 3 Bits	CFI 1 Bit	VLAN ID 12 bits

7.1.1 Forwarding Tagged and Untagged Frames

Each port on the switch is capable of passing tagged or untagged frames. To forward a frame from an 802.1Q VLAN-aware switch to an 802.1Q VLAN-unaware switch, the switch first decides where to forward the frame and then strips off the VLAN tag. To forward a frame from an 802.1Q VLAN-unaware switch to an 802.1Q VLAN-aware switch, the switch first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID. The default PVID is VLAN 1 for all ports, but this can be changed.

7.1.2 Automatic VLAN Registration

GARP and GVRP are the protocols used to automatically register VLAN membership across switches.

GARP

GARP (Generic Attribute Registration Protocol) allows network switches to register and de-register attribute values with other GARP participants within a bridged LAN. GARP is a protocol that provides a generic mechanism for protocols that serve a more specific application, for example, GVRP.

GARP Timers

Switches join VLANs by making a declaration. A declaration is made by issuing a Join message using GARP. Declarations are withdrawn by issuing a Leave message. A Leave All message terminates all registrations. GARP timers set declaration timeout values.

GVRP

GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Enable this function to permit VLANs groups beyond the local switch.

Please refer to the following table for common GARP terminology.

Table 7-1 GARP Terminology

VLAN PARAMETER	TERM	DESCRIPTION
VLAN Type	Permanent VLAN	This is a static VLAN created manually.
	Dynamic VLAN	This is a VLAN configured by a GVRP registration/deregistration process.
VLAN Administrative Control	Registration Fixed	Fixed registration ports are permanent VLAN members.
	Registration Forbidden	Ports with registration forbidden are forbidden to join the specified VLAN.
	Normal Registration	Ports dynamically join a VLAN using GVRP.
VLAN Tag Control	Tagged	Ports belonging to the specified VLAN tag all outgoing frames transmitted.
	Untagged	Ports belonging to the specified don't tag all outgoing frames transmitted.
VLAN Port	Port VID	This is the VLAN ID assigned to untagged frames that this port received.
	Acceptable frame type	You may choose to accept both tagged and untagged incoming frames or just tagged incoming frames on a port.
	Ingress filtering	If set, the switch discards incoming frames for VLANs that do not have this port as a member

7.1.3 Port VLAN Trunking

Enable **VLAN Trunking** on a port to allow frames belonging to unknown VLAN groups to pass through that port. This is useful if you want to set up VLAN groups on end devices without having to configure the same VLAN groups on intermediary devices.

Refer to the following figure. Suppose you want to create VLAN groups 1 and 2 (V1 and V2) on devices A and B. Without **VLAN Trunking,** you must configure VLAN groups 1 and 2 on all intermediary switches C, D and E; otherwise they will drop frames with unknown VLAN group tags. However, with **VLAN Trunking** enabled on a port(s) in each intermediary switch you only need to create VLAN groups in the end devices (A and B). C, D and E automatically allow frames with VLAN group tags 1 and 2 (VLAN groups that are unknown to those switches) to pass through their VLAN trunking port(s).

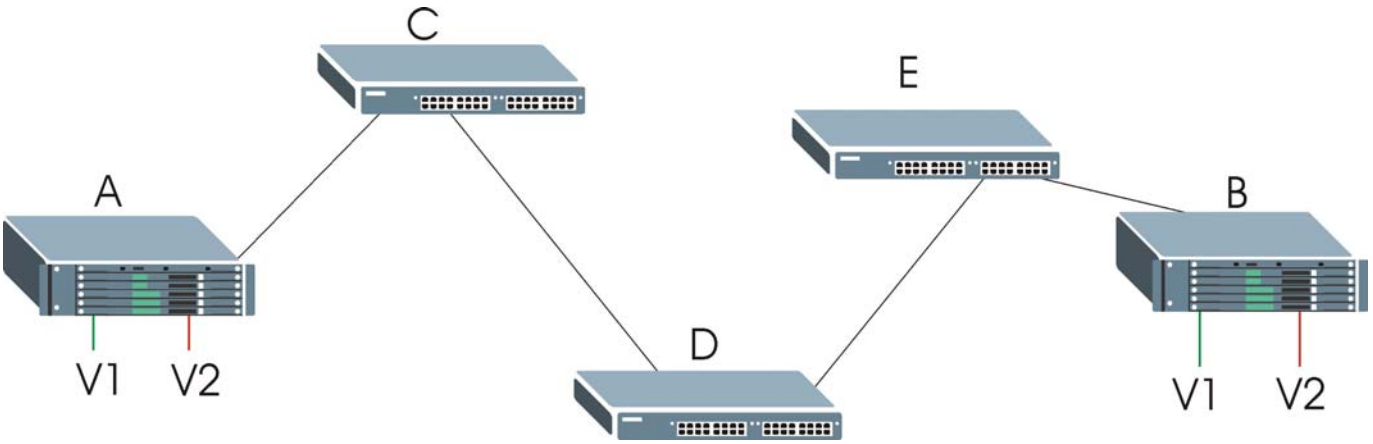


Figure 7-1 Port VLAN Trunking

7.1.4 Select VLAN Type

Follow the steps below to select the VLAN type on the switch.

Step 1. Select **802.1Q** as the **VLAN Type** in the **Switch Setup** screen (under **Basic Setting**) and click **Apply**.

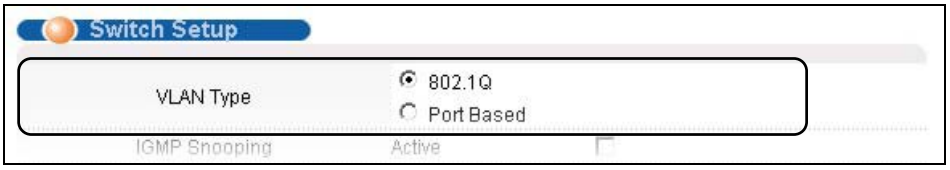


Figure 7-2 Switch Setup: VLAN Type

Step 2. Click **Advanced Application**, **VLAN** from the navigation panel to display the **VLAN Status** screen as shown next.

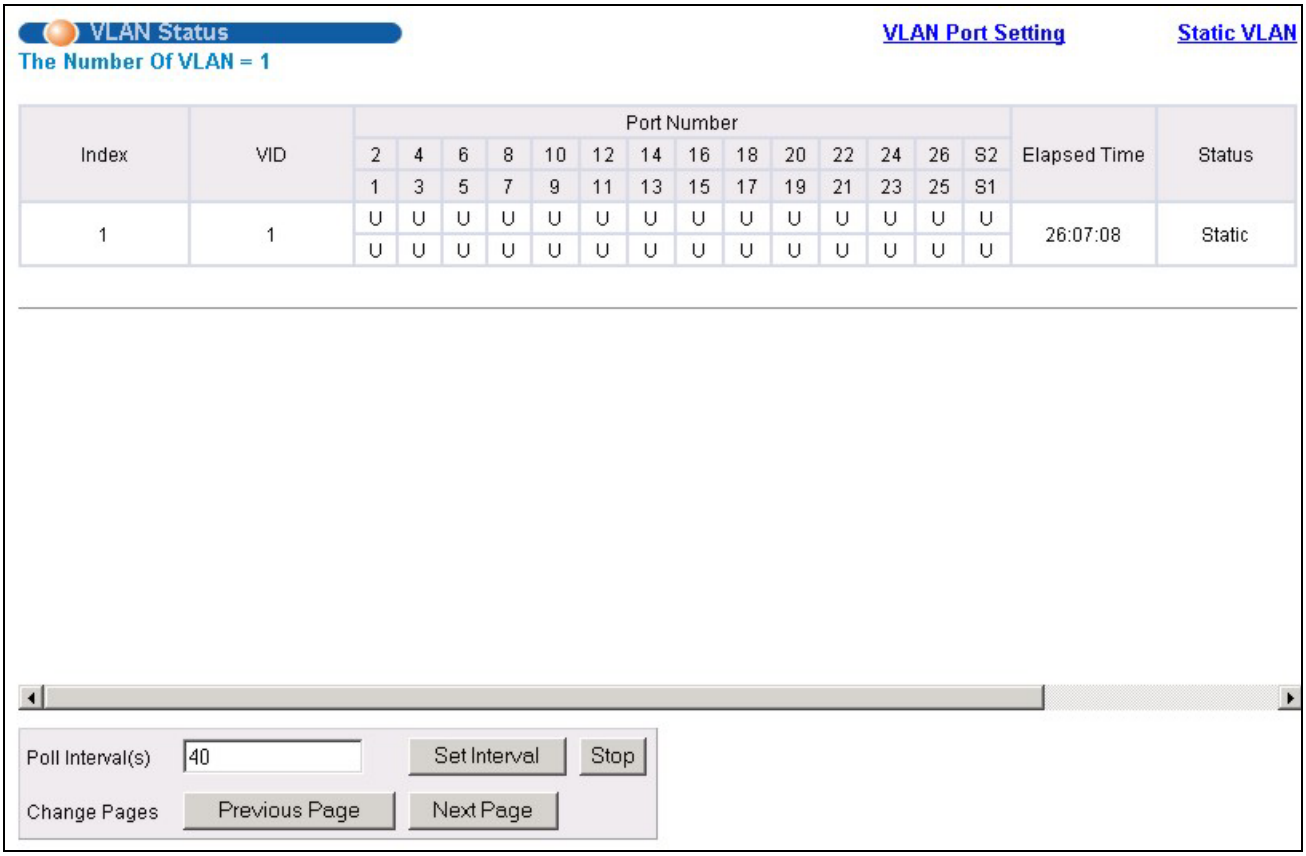


Figure 7-3 Advanced: VLAN Status

The following table describes the labels in this screen.

Table 7-2 Advanced: VLAN Status

LABEL	DESCRIPTION
The Number of VLAN	This is the number of VLANs configured on the switch.
Index	This is the VLAN index number.
VID	This is the VLAN identification number that was configured in the **VLAN Setup** screen.
Port Number	This column displays the ports that are participating in a VLAN. A tagged port is marked as **T**, an untagged port is marked as **U** and ports not participating in a VLAN in marked as "**–**".
Elapsed Time	This field shows how long it has been since a normal VLAN was registered or a static VLAN was set up.
Status	This field shows how this VLAN was added to the switch; dynamically using GVRP or statically, that is, added as a permanent entry.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt polling statistics.

Table 7-2 Advanced: VLAN Status

LABEL	DESCRIPTION
Change Pages	Click **Previous Page** or **Next Page** to show the previous/next screen if all status information cannot be seen in one screen.

7.1.5 Configuring VLAN Port Settings

To configure the VLAN settings on a port, click the **VLAN Port Setting** link in the **VLAN Status** screen.

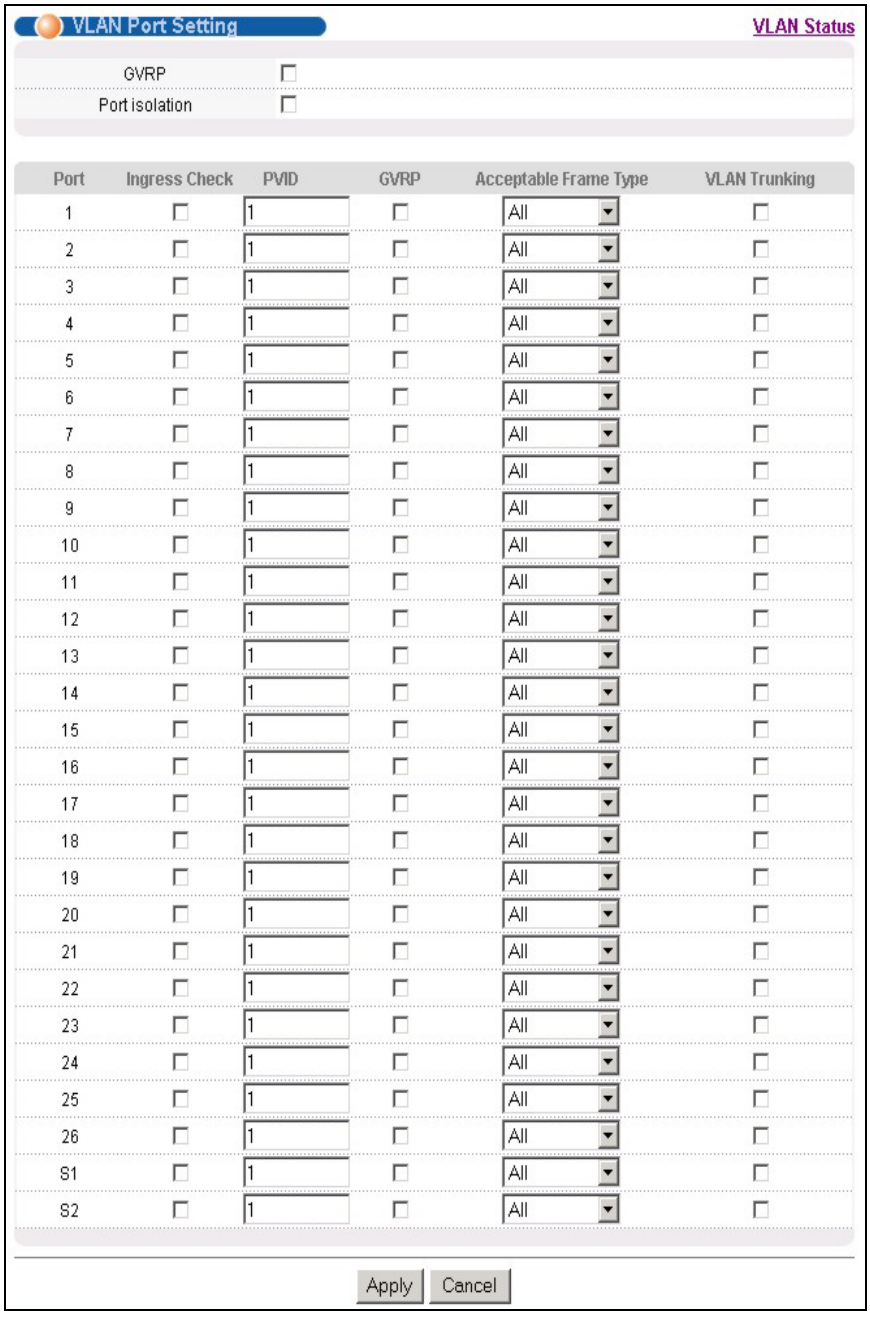


Figure 7-4 VLAN: VLAN Port Setting

The following table describes the labels in this screen.

Table 7-3 VLAN: VLAN Port Setting

LABEL	DESCRIPTION
GVRP	GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Select this check box to permit VLAN groups beyond the local switch.
Port Isolation	**Port Isolation** allows each port (1 to 26) to communicate only with the CPU management port but not communicate with each other. All incoming ports are selected while only the CPU outgoing port is selected. This option is the most limiting but also the most secure.
Port	This field displays the port numbers.
Ingress Check	Select this check box to activate ingress filtering. Clear this check box to disable ingress filtering.
PVID	Enter a number between 1 and 4094 as the port VLAN ID.
GVRP	Select this check box to allow GVRP on this port.
Acceptable Frame Type	Specify the type of frames allowed on a port. Choices are **All**, **Tag Only** and **Untag Only**. Select **All** from the drop-down list box to accept all untagged or tagged frames on this port. This is the default setting. Select **Tag Only** to accept only tagged frames on this port. All untagged frames will be dropped. Select **Untag Only** to accept only untagged frames on this port. All tagged frames will be dropped.
VLAN Trunking	Enable **VLAN Trunking** on ports connected to other switches or routers (but not ports directly connected to end users) to allow frames belonging to unknown VLAN groups to pass through the switch.
Apply	Click **Apply** to save the changes
Cancel	Click **Cancel** to start configuring the screen again.

7.1.6 Configuring a VLAN

To configure a new VLAN, click **Static VLAN** in the **VLAN Status** screen to display the screen as shown next.

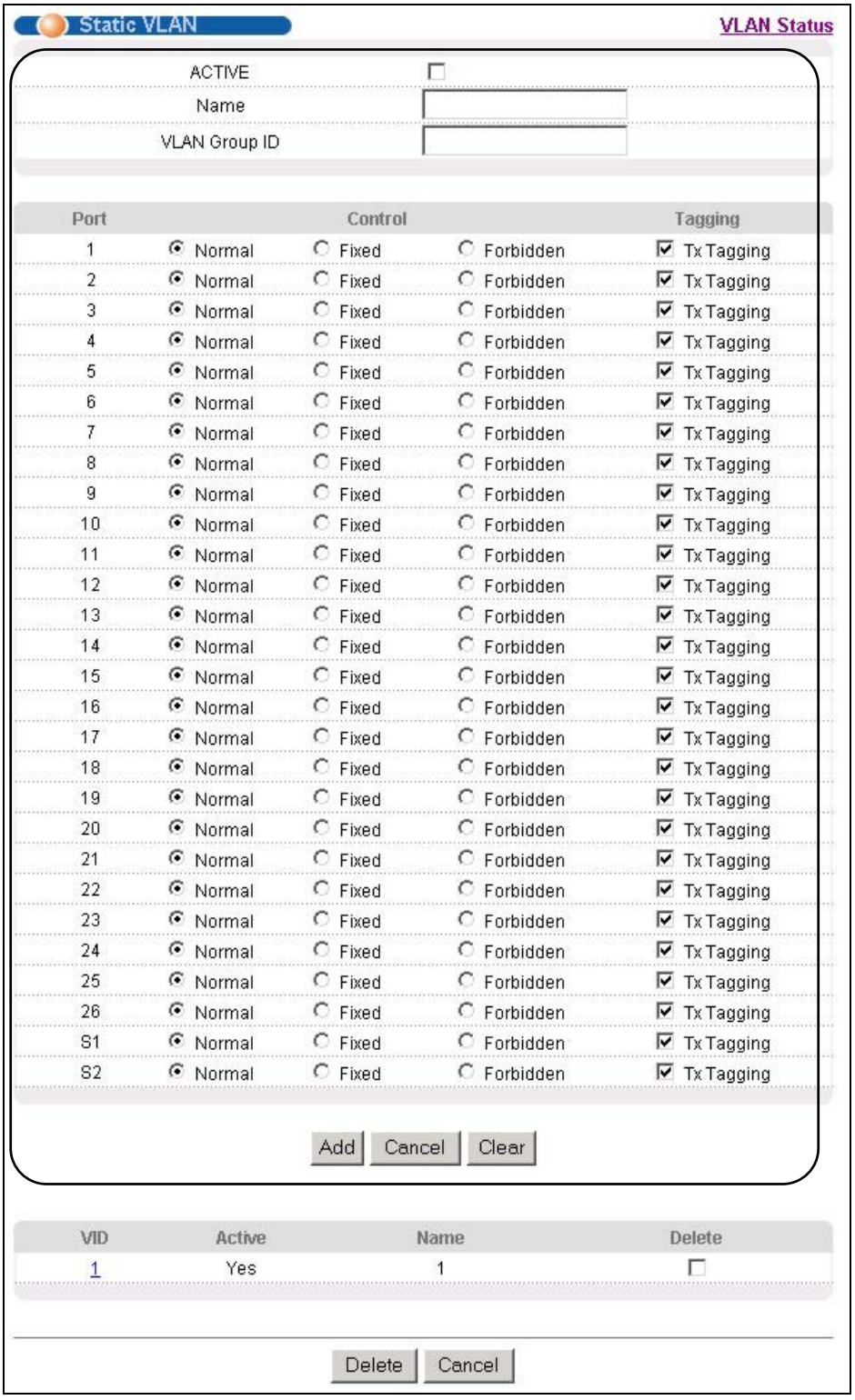


Figure 7-5 VLAN: Static VLAN

The following table describes the labels in this screen.

Table 7-4 VLAN: Static VLAN

LABEL	DESCRIPTION
ACTIVE	Select this check box to activate the VLAN settings.
Name	Enter a descriptive name for the VLAN group for identification purposes.
VLAN Group ID	Enter the VLAN ID for this static entry; the valid range is between 1 and 4094.
Port	The port number identifies the port you are configuring. Ports 25 and 26 are the uplink ports.
Control	Select **Normal** for the port to dynamically join this VLAN group using GVRP. This is the default selection. Select **Fixed** for the port to be a permanent member of this VLAN group. Select **Forbidden** if you want to prohibit the port from joining this VLAN group.
Tagging	Select **TX Tagging** if you want the port to tag all outgoing frames transmitted with this VLAN Group ID.
Add	Click **Add** to add the settings as a new entry in the summary table below.
Cancel	Click **Cancel** to reset the fields.
Clear	Click **Clear** to start configuring the screen again.

7.1.7 Viewing and Editing VLAN Settings

To view a summary of the VLAN configuration, scroll down to the summary table at the bottom of the **Static VLAN** screen.

To change the settings of a rule, click a number in the **Index** field.

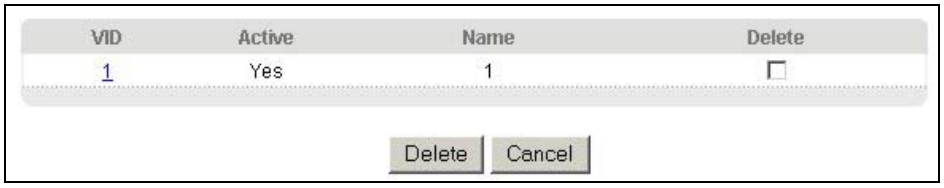


Figure 7-6 Static VLAN: Summary Table

The following table describes the labels in the summary table.

Table 7-5 Static VLAN: Summary Table

LABEL	DESCRIPTION
VID	This field displays the ID number of the VLAN group. Click the number to edit the VLAN settings.
Active	This field indicates whether the VLAN settings are enabled (**Yes**) or disabled (**No**).
Name	This field displays the descriptive name for this VLAN group.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

7.2 Introduction to Port-based VLANs

Port-based VLANs are VLANs where the packet forwarding decision is based on the destination MAC address and its associated port.

Port-based VLANs require allowed outgoing ports to be defined for each port. Therefore, if you wish to allow two subscriber ports to talk to each other, for example, between conference rooms in a hotel, you must define the egress (an egress port is an outgoing port, that is, a port through which a data packet leaves) for both ports.

Port-based VLANs are specific only to the switch on which they were created.

When you activate port-based VLAN, the ES uses a default VLAN ID of 1. You cannot change it.

In screens (such as IP Setup **and** Filtering**) that require a VID, you must enter 1 as the VID.**

The port-based VLAN setup screen is shown next. The **CPU** management port forms a VLAN with all Ethernet ports.

7.2.1 Configuring a Port-based VLAN

Select **Port Based** as the **VLAN Type** in the **Switch Setup** screen (see *Figure 7-2*) and then click **VLAN** from the navigation panel to display the next screen.

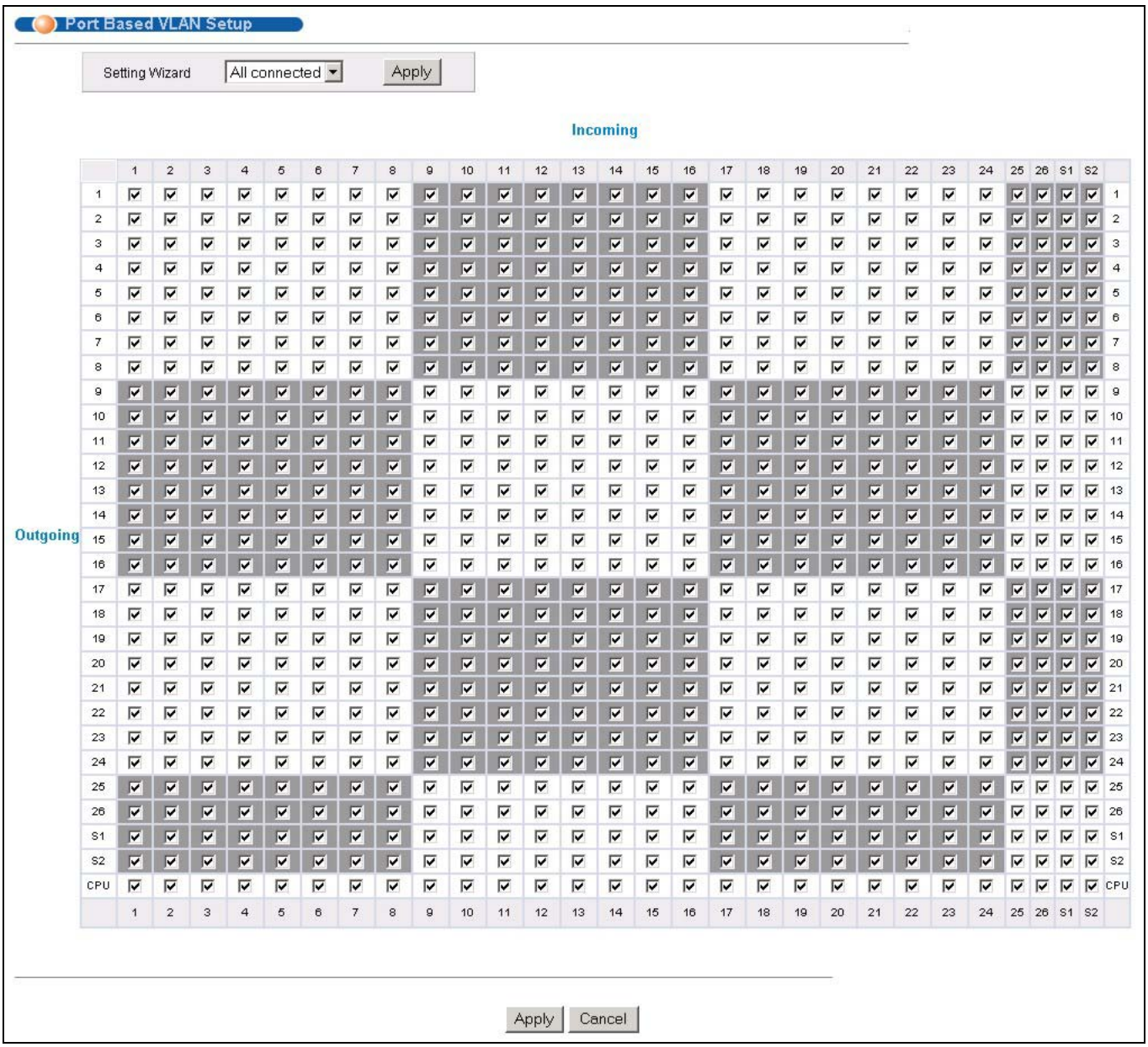


Figure 7-7 Port Based VLAN Setup (All Connected)

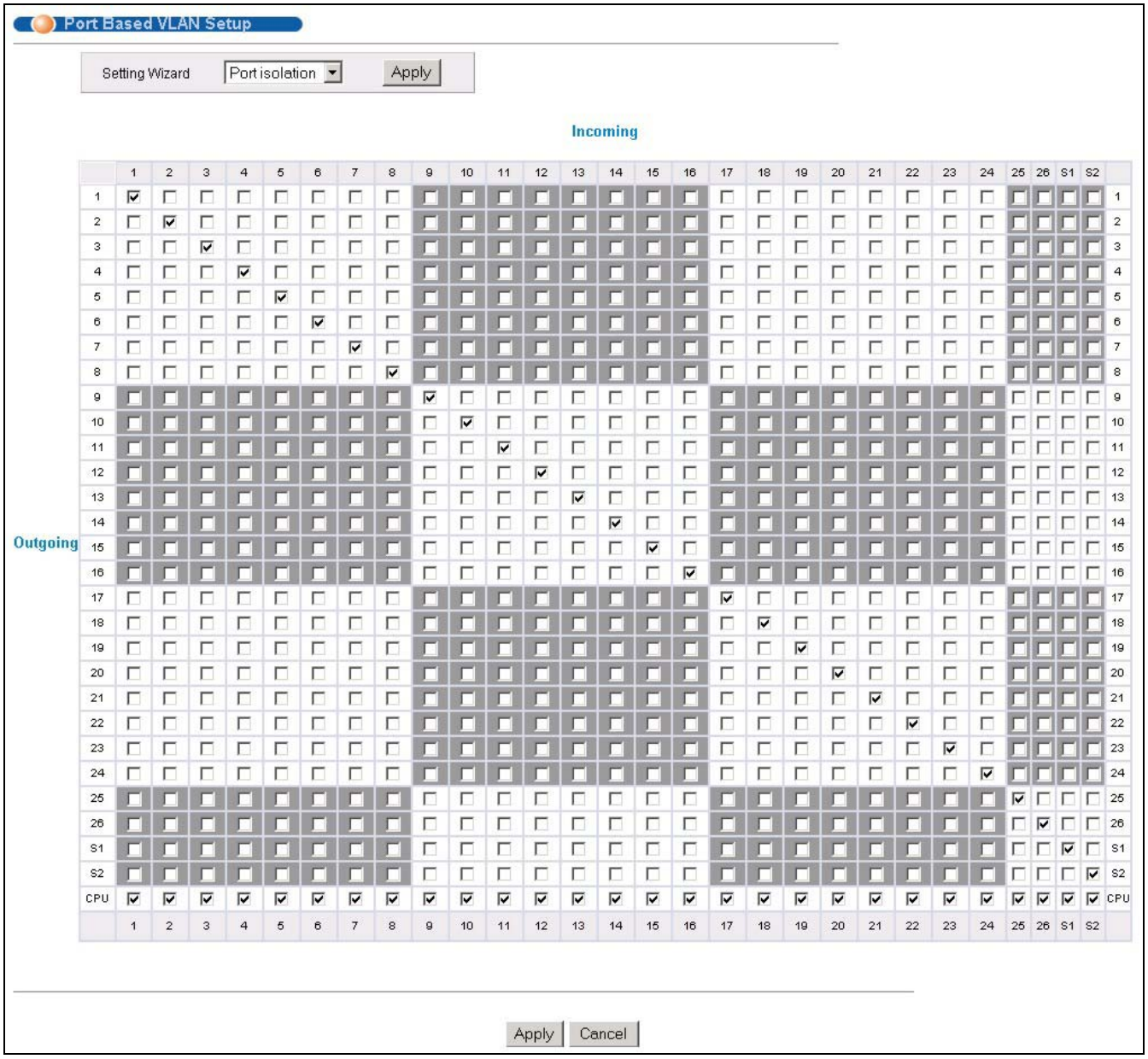


Figure 7-8 Port Based VLAN Setup (Port Isolation)

The following table describes the labels in this screen.

Table 7-6 Port Based VLAN Setup

LABEL	DESCRIPTION
Setting Wizard	Choose from **All connected** or **Port isolation**. **All connected** means all ports can communicate with each other, that is, there are no virtual LANs. All incoming and outgoing ports are selected (*Figure 7-7*). This option is the most flexible but also the least secure. **Port isolation** means that each port can only communicate with the CPU management port and cannot communicate with each other. All incoming ports are selected while only the CPU outgoing port is selected (*Figure 7-8*). This option is the most limiting but also the most secure. After you make your selection, click **Apply** (top right of screen) to display the screens as mentioned above. You can still customize these settings by adding/deleting incoming or outgoing ports, but you must also click **Apply** at the bottom of the screen.
Incoming	These are the ingress ports; an ingress port is an incoming port, that is, a port through which a data packet enters. If you wish to allow two subscriber ports to talk to each other, you must define the ingress port for both ports. The numbers in the top row denote the incoming port for the corresponding port listed on the left (its outgoing port). **CPU** refers to the switch management port. By default it forms a VLAN with all Ethernet ports. If it does not form a VLAN with a particular port then the switch cannot be managed from that port.
Outgoing	These are the egress ports; an egress port is an outgoing port, that is, a port through which a data packet leaves. If you wish to allow two subscriber ports to talk to each other, you must define the egress port for both ports. **CPU** refers to the switch management port. By default it forms a VLAN with all Ethernet ports. If it does not form a VLAN with a particular port then the switch cannot be managed from that port.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to start configuring the screen again.

Chapter 8
Static MAC Forward Setup

Use these screens to configure static MAC address forwarding.

8.1 Introduction to Static MAC Forward Setup

A static MAC address is an address that has been manually entered in the MAC address learning table. Static MAC addresses do not age out. When you set up static MAC address rules, you are setting static MAC addresses for a port. This may reduce the need for broadcasting.

8.2 Configuring Static MAC Forwarding

Click **Advanced Applications, Static MAC Forwarding** in the navigation panel to display the configuration screen as shown.

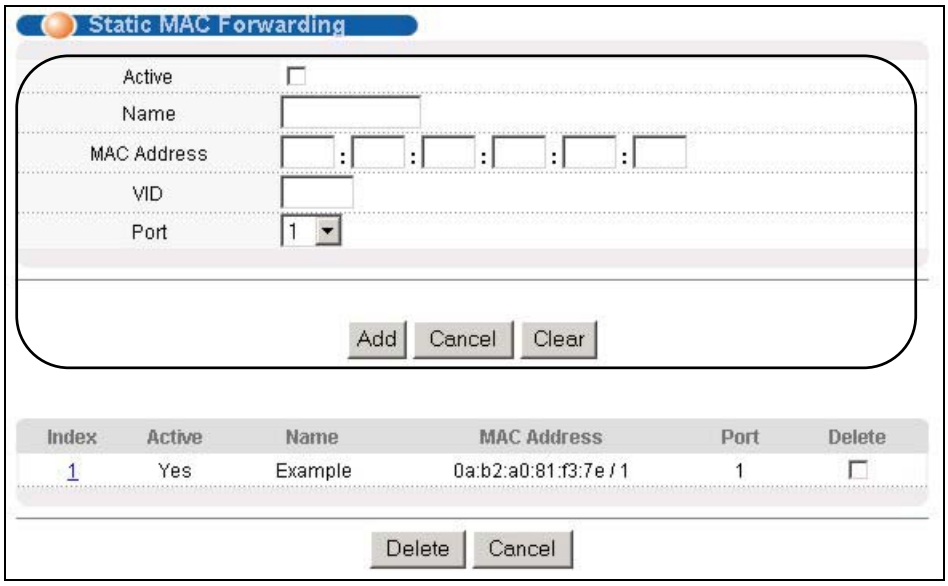


Figure 8-1 Advanced: Static MAC Forwarding

The following table describes the labels in this screen.

Table 8-1 Advanced: Static MAC Forwarding

LABEL	DESCRIPTION
Active	Select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by clearing this check box.
Name	Enter a descriptive name for identification purposes for this static MAC address forwarding rule.
MAC Address	Enter the MAC address in valid MAC address format, that is, six hexadecimal character pairs. Static MAC addresses do not age out.

Table 8-1 Advanced: Static MAC Forwarding

LABEL	DESCRIPTION
VID	Enter the VLAN identification number.
Port	Select a port where the MAC address entered in the previous field will be automatically forwarded.
Add	After you set the fields above, click **Add** to insert a new rule.
Cancel	Click **Cancel** to reset the fields.
Clear	Click **Clear** to begin configuring this screen afresh.

8.3 Viewing and Editing Static MAC Forwarding Rules

To view a summary of the rule configuration, scroll down to the summary table at the bottom of the **Static MAC Forwarding** screen.

To change the settings of a rule, click a number in the **Index** field.

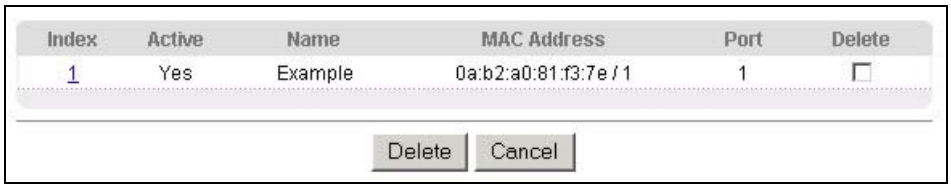


Figure 8-2 Static MAC Forwarding: Summary Table

The following table describes the labels in the summary table.

Table 8-2 Static MAC Forwarding: Summary Table

LABEL	DESCRIPTION
Index	Click an index number to modify a static MAC address rule for a port.
Active	This field displays whether this static MAC address forwarding rule is active (**Yes**) or not (**No**). You may temporarily deactivate a rule without deleting it.
Name	This field displays the descriptive name for identification purposes for this static MAC address-forwarding rule.
MAC Address	This field displays the MAC address that will be forwarded and the VLAN identification number to which the MAC address belongs.
Port	This field displays the port where the MAC address shown in the next field will be forwarded.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

Chapter 9 Filtering

This chapter discusses static IP and MAC address port filtering.

9.1 Introduction to Filtering

Port filtering means sifting traffic from one or all ports to one or all ports based on the source and/or destination IP and/or MAC addresses and VLAN group.

9.1.1 Note About Configuration

The following rules apply when configuring filtering.

- The rule applies to traffic flowing in both directions if both a source and destination are specified.
- The rule applies to traffic flowing in one direction if either a source or destination is specified.
- No any-to-any rules are allowed. That is, you cannot select **Ignore** for both the source and destination ports.
- No blank rules are allowed. If you do not select **Ignore**, you must set the related fields.

9.2 Configuring a Filtering Rule

Click **Advanced Application**, **Filtering** in the navigation panel to display the screen as shown next.

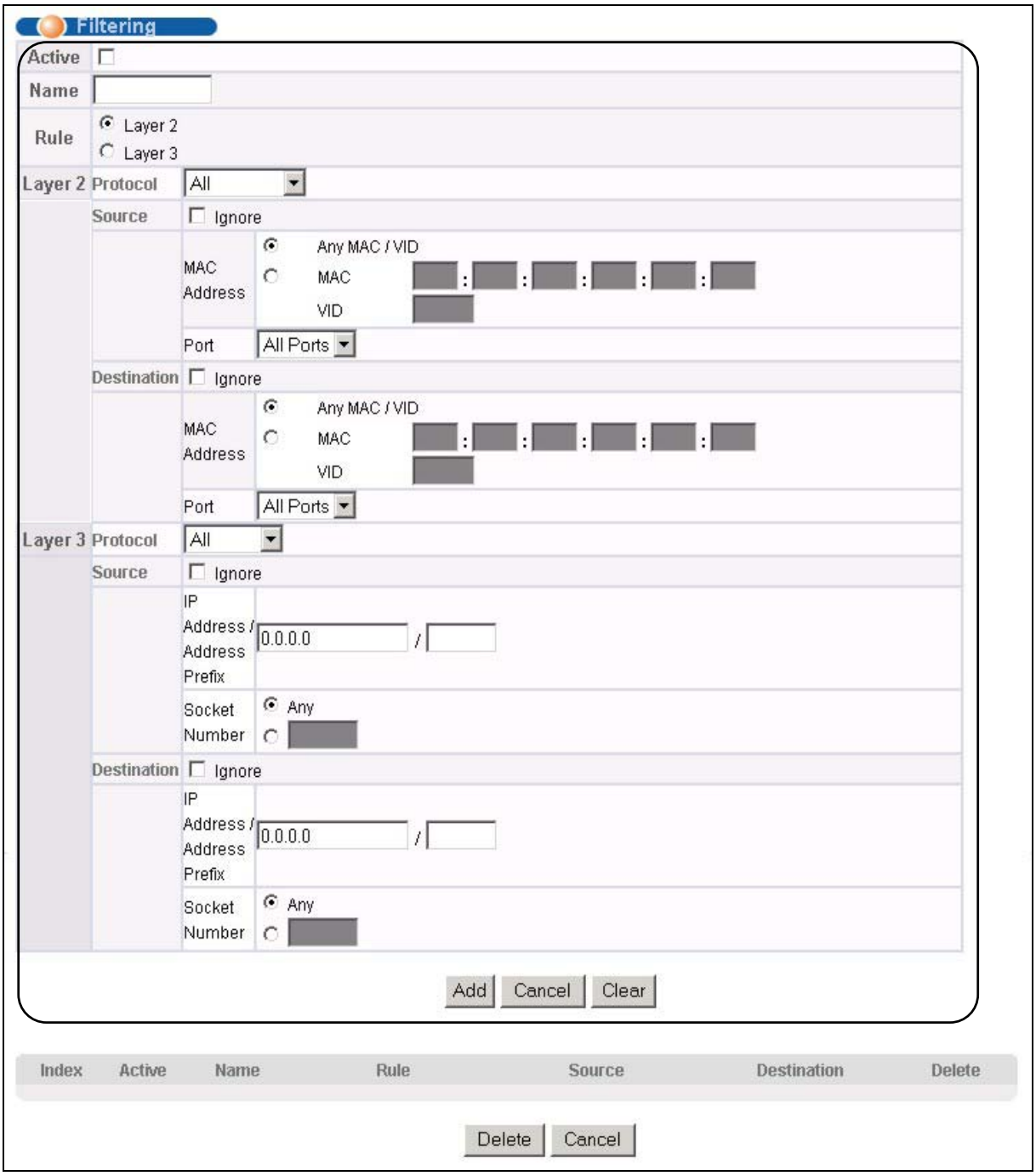


Figure 9-1 Filtering

The following table describes the related labels in this screen.

Table 9-1 Filtering

LABEL	DESCRIPTION
Active	Make sure to select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by deselecting this check box.

Table 9-1 Filtering

LABEL	DESCRIPTION
Name	Type a descriptive name for this rule. This is for identification purpose only.
Rule	Specify to which network layer (**Layer 2** or **Layer 3**) this rule applies.
Layer 2 Set the related fields when you select **Layer 2** in the **Rule** field.	
The VID for the source and destination must be the same.	
Protocol	Select the protocol traffic to which this rule applies.
Source	The next three fields pertain to the source MAC address and source port.
Ignore	Click this check box to ignore any traffic from all source ports.
MAC Address	Select **Any MAC/VID** to apply the rule to all MAC address and VLAN group identification numbers. To specify a source, select the second choice and type a MAC address in valid MAC address format (six hexadecimal character pairs) and then enter the VLAN group identification number.
Port	Select the port to which the rule should be applied. You may choose one port only or all ports (**All Ports**).
Destination	The next three fields pertain to the destination MAC address and destination port.
Ignore	Click this check box to ignore any traffic to all destination ports.
MAC Address	Select **Any MAC/VID** to apply the rule to all MAC address and VLAN group identification numbers. To specify a destination, select the second choice and type a MAC address in valid MAC address format (six hexadecimal character pairs) and then enter the VLAN group identification number.
Port	Select the port to which the rule should be applied. You may choose one port only or all ports (**All Ports**).
Layer 3 Set the related fields below when you select **Layer 3** in the **Rule** field.	
Protocol	Select the protocol traffic to which this rule applies.
Source	The next three fields pertain to the source IP address and source port.
Ignore	Click this check box to ignore any traffic from all source ports.
IP Address/Address Prefix	Enter a source IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask.

Table 9-1 Filtering

LABEL	DESCRIPTION
Socket Number	**You *must* set the** IP Address/Address Prefix **fields and select either** UDP **or** TCP **in the** Protocol **field before you can configure the socket number.**
	Select **Any** to apply to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number.
Destination	The next three fields pertain to the destination IP address and destination port.
Ignore	Click this check box to ignore any traffic to all destination ports.
IP Address/Address Prefix	Enter a destination IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask.
Socket Number	**You *must* set the** IP Address/Address Prefix **fields and select either** UDP **or** TCP **in the** Protocol **field before you can configure the socket number.**
	Select **Any** to apply to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number.
Add	Click **Add** to inset the entry to the summary table below.
Cancel	Click **Cancel** to reset the fields back to your previous configuration.
Clear	Click **Clear** to set the above fields back to the factory defaults.

9.3 Viewing and Editing Filter Rules

To view a summary of the rule configuration, scroll down to the summary table at the bottom of the **Filtering** screen. To change the settings of a rule, click a number in the **Index** field.

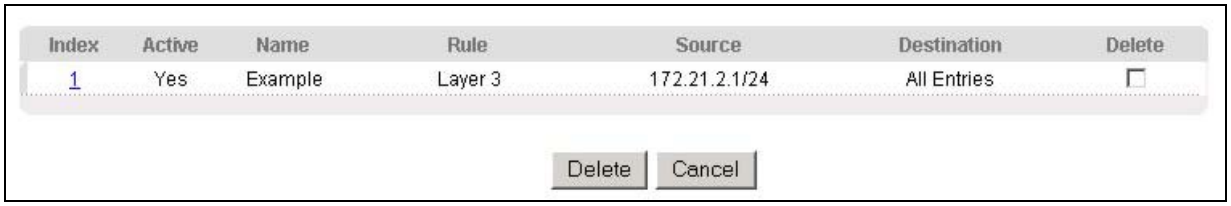


Figure 9-2 Filtering: Summary Table

The following table describes the labels in the summary table.

Table 9-2 Filtering: Summary Table

LABEL	DESCRIPTION
Index	This field displays the index number of the rule. Click an index number to edit the rule.
Active	This field displays **Yes** when the rule is activated and **No** when is it deactivated.
Name	This field displays the descriptive name for this rule. This is for identification purpose only.

Table 9-2 Filtering: Summary Table

LABEL	DESCRIPTION
Rule	This field displays the network layer (**Layer 2** or **Layer 3**) to which this rule applies.
Source	For **Layer 2** rules, this field displays the source port number, the source MAC address with the VLAN identification number to which the MAC address belongs or a combination of the two. For **Layer 3** rules, this field displays the source protocol socket number, the source IP address and address prefix or a combination of the two. **All Entries** means all IP/MAC addresses from all ports.
Destination	For **Layer 2** rules, this field displays the destination port number, the destination MAC address with the VLAN identification number to which the MAC address belongs or a combination of the two. For **Layer 3** rules, this field displays the source protocol socket number, the source IP address and address prefix or a combination of the two. **All Entries** means all IP/MAC addresses from all ports.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

Chapter 10
Spanning Tree Protocol

This chapter introduces the Spanning Tree Protocol (STP).

10.1 Introduction to Spanning Tree Protocol (STP)

STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a switch to interact with other STP-compliant switches in your network to ensure that only one route exists between any two stations on the network.

10.1.1 STP Terminology

The root bridge is the base of the spanning tree; it is the bridge with the lowest identifier value (MAC address).

Path cost is the cost of transmitting a frame onto a LAN through that port. It is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost - see the next table.

Table 10-1 STP Path Costs

	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	4Mbps	250	100 to 1000	1 to 65535
Path Cost	10Mbps	100	50 to 600	1 to 65535
Path Cost	16Mbps	62	40 to 400	1 to 65535
Path Cost	100Mbps	19	10 to 60	1 to 65535
Path Cost	1Gbps	4	3 to 10	1 to 65535
Path Cost	10Gbps	2	1 to 5	1 to 65535

On each bridge, the root port is the port through which this bridge communicates with the root. It is the port on this switch with the lowest path cost to the root (the root path cost). If there is no root port, then this switch has been accepted as the root bridge of the spanning tree network.

For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

10.1.2 How STP Works

After a bridge determines the lowest cost-spanning tree with STP, it enables the root port and the ports that are the designated ports for connected LANs, and disables all other ports that participate in STP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

STP-aware switches exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

10.1.3 STP Port States

STP assigns five port states (see next table) to eliminate packet looping. A bridge port is not allowed to go directly from blocking state to forwarding state so as to eliminate transient loops.

Table 10-2 STP Port States

PORT STATE	DESCRIPTION
Disabled	STP is disabled (default).
Blocking	Only configuration and management BPDUs are received and processed.
Listening	All BPDUs are received and processed.
Learning	All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded.
Forwarding	All BPDUs are received and processed. All information frames are received and forwarded.

10.2 STP Status

Click **Advanced Application**, **Spanning Tree Protocol** in the navigation panel to display the status screen as shown next.

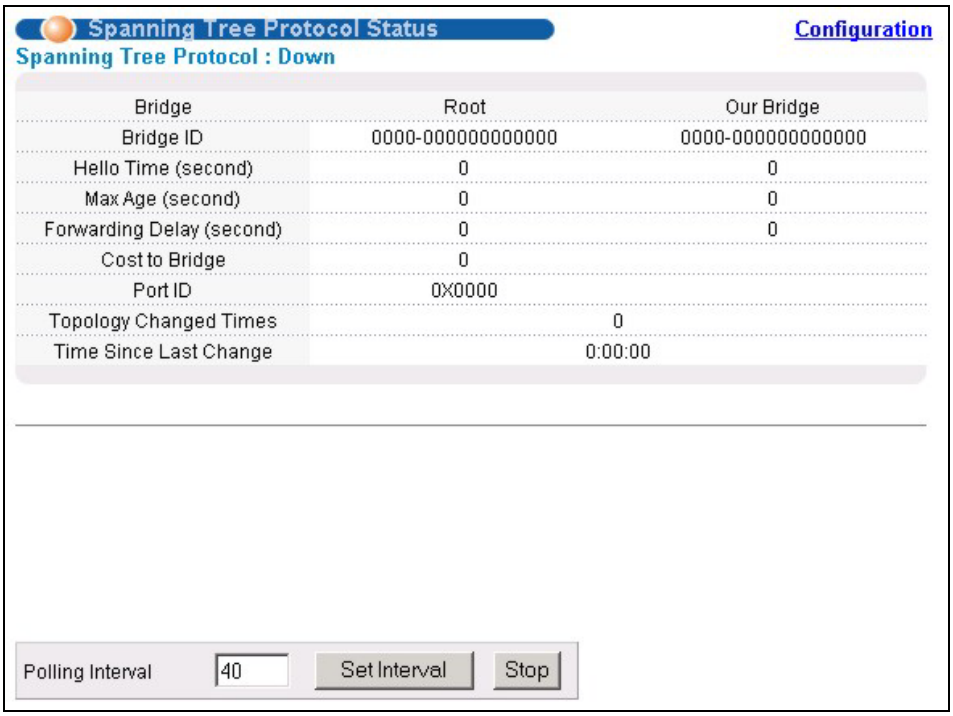


Figure 10-1 Spanning Tree Protocol: Status

The following table describes the labels in this screen.

Table 10-3 Spanning Tree Protocol: Status

LABEL	DESCRIPTION
Spanning Tree Protocol	This field displays **Running** if STP is activated. Otherwise, it displays **Down**.
Configuration	Click **Configuration** to configure STP settings. Refer to *Section 10.2.1*.
Bridge	**Root** refers to the base of the spanning tree (the root bridge). **Our Bridge** is this switch. This switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for **Root** and **Our Bridge** if the switch is the root switch.
Hello Time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines **Hello Time, Max Age** and **Forwarding Delay**
Max Age (second)	This is the maximum time (in seconds) a switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding).
Cost to Bridge	This is the path cost from the root port on this switch to the root switch.
Port ID	This is the priority and number of the port on the switch through which this switch must communicate with the root of the Spanning Tree.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt STP statistic polling.

10.2.1 Configuring STP

To configure STP, click the **Configuration** link in the **Spanning Tree Protocol** screen as shown next.

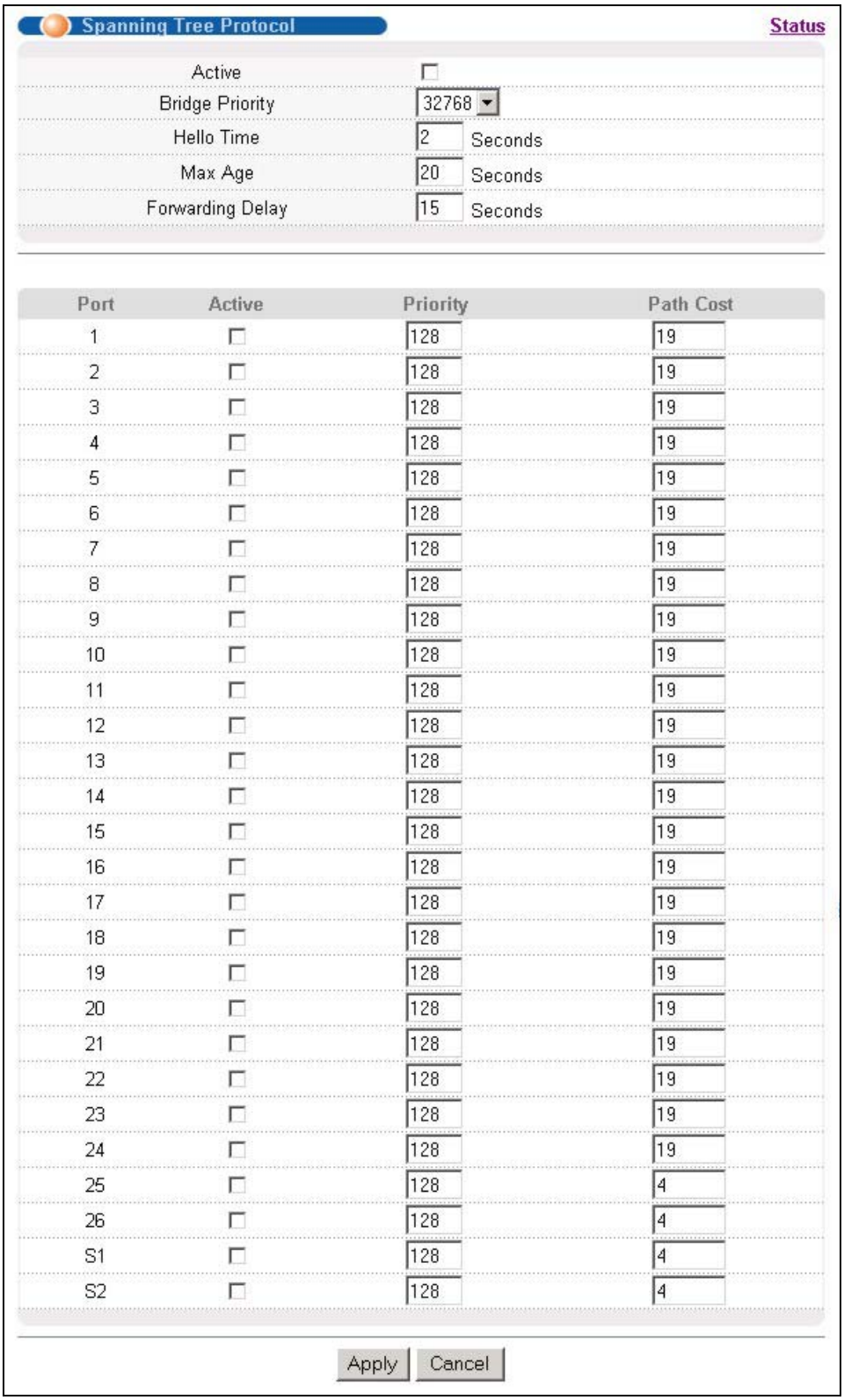


Figure 10-2 Spanning Tree Protocol: Configuration

The following table describes the labels in this screen.

Table 10-4 Spanning Tree Protocol: Configuration

LABEL	DESCRIPTION
Status	Click **Status** to display the **Spanning Tree Protocol Status** screen (see *Figure 10-1*).
Active	Select this check box to activate STP. Clear this checkbox to disable STP.
Bridge Priority	Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Select a value from the drop-down list box. The lower the numeric value you assign, the higher the priority for this bridge. Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
Max Age	This is the maximum time (in seconds) a switch can wait without receiving a BPDU before attempting to reconfigure. All switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the switch ports attached to the network. The allowed range is 6 to 40 seconds.
Forwarding Delay	This is the maximum time (in seconds) a switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: **2 * (Forward Delay - 1) >= Max Age >= 2 * (Hello Time + 1)**
Port	This field displays the port number.
Active	Select this check box to activate STP on this port.
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is assigned according to the speed of the bridge. The slower the media, the higher the cost - see *Table 10-1* for more information.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Chapter 11 Bandwidth Control

This chapter shows you how you can cap the maximum bandwidth allowed from specific source(s) to specified destination(s) using the Bandwidth Control setup screen.

11.1 Introduction to Bandwidth Control

Bandwidth control means defining a maximum allowable bandwidth for traffic flows from specified source(s) to specified destination(s). Click **Advanced Application**, **Bandwidth Control** in the navigation panel to bring up the screen as shown next.

11.1.1 Note About Configuration

The following rules apply when configuring bandwidth control.

- The rule applies to traffic flowing in both directions if both a source and destination are specified.
- The rule applies to traffic flowing in one direction if either a source or destination is specified.
- No any-to-any rules are allowed, that is, you cannot select **Ignore** for both the source and destination ports.
- No port-to-port rules are allowed, that is, you cannot set the switch to perform bandwidth management between two ports on the same switch.
- No blank rules allowed. If you do not select **Ignore**, you must set the related fields.

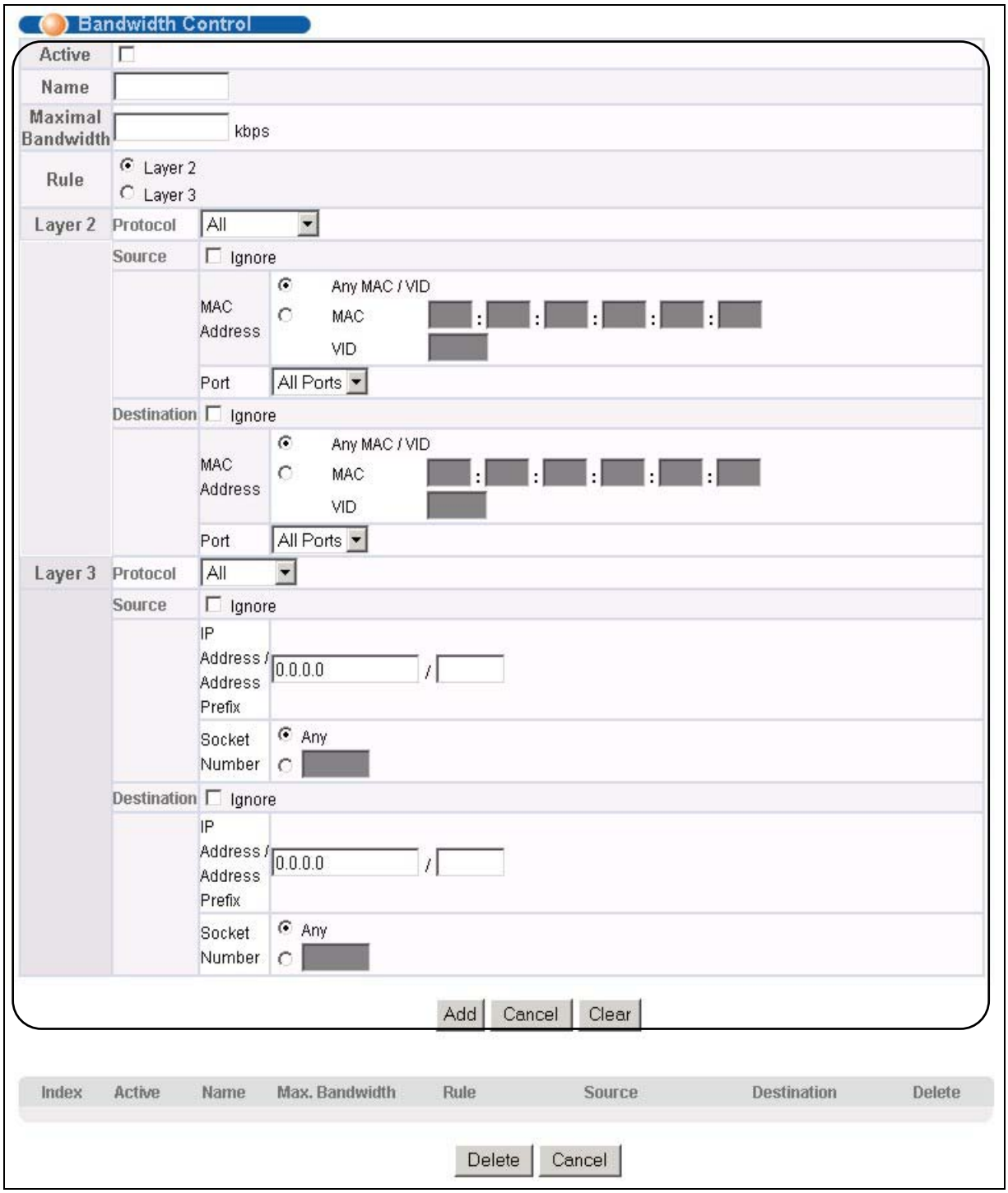


Figure 11-1 Advanced: Bandwidth Control

The following table describes the labels in this screen.

Table 11-1 Advanced: Bandwidth Control

LABEL	DESCRIPTION
Active	Make sure to select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by deselecting this check box.
Name	Type a descriptive name for this rule. This is for identification purpose only.
Maximum Bandwidth	Type the maximum bandwidth allowed in kilobits per second (kbps) for this traffic flow.
Rule	Specify to which network layer (**Layer 2** or **Layer 3**) this rule applies.
Layer 2 Set the related fields when you select **Layer 2** in the **Rule** field.	
The VID for the source and destination must be the same. No port-to-MAC or MAC-to-port rules are allowed.	
Protocol	Select the protocol traffic to which this rule applies.
Source	The next three fields pertain to the source MAC address and source port.
Ignore	Click this check box to ignore any traffic from all source ports.
MAC Address	Select **Any MAC/VID** to apply the rule to all MAC address and VLAN group identification numbers. To specify a source, select the second choice and type a MAC address in valid MAC address format (six hexadecimal character pairs) and then enter the VLAN group identification number.
Port	Select the port to which the rule should be applied. You may choose one port only or all ports (**All Ports**).
Destination	The next three fields pertain to the destination MAC address and destination port.
Ignore	Click this check box to ignore any traffic to all destination ports.
MAC Address	Select **Any MAC/VID** to apply the rule to all MAC address and VLAN group identification numbers. To specify a destination, select the second choice and type a MAC address in valid MAC address format (six hexadecimal character pairs) and then enter the VLAN group identification number.
VID	Type the VLAN group identification number.
Port	Select the port to which the rule should be applied. You may choose one port only or all ports (**All Ports**).
Layer 3 Set the related fields below when you select **Layer 3** in the **Rule** field.	
Protocol	Select the protocol traffic to which this rule applies.
Source	The next three fields pertain to the source IP address and source port.

Table 11-1 Advanced: Bandwidth Control

LABEL	DESCRIPTION
Ignore	Click this check box to ignore any traffic from all source ports.
IP Address/Address Prefix	Enter a source IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the octet.
Socket Number	**You *must* set the** IP Address/Address Prefix **fields and select either** UDP **or** TCP **in the** Protocol **field before you can configure the socket number.**
	Select **Any** to apply to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number.
Destination	The next three fields pertain to the destination IP address and destination port.
Ignore	Click this check box to ignore any traffic to all destination ports.
IP Address/Address Prefix	Enter a destination IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the octet.
Socket Number	**You *must* set the** IP Address/Address Prefix **fields and select either** UDP **or** TCP **in the** Protocol **field before you can configure the socket number.**
	Select **Any** to apply to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number.
Add	Click **Add** to inset the entry to the summary table below.
Cancel	Click **Cancel** to reset the fields back to your previous configuration.
Clear	Click **Clear** to reset the fields back to the factory defaults.

11.1.2 VLAN Bandwidth Control

The ES supports bandwidth control on a source VLAN. To configure bandwidth control on a VLAN, create a layer 2 rule and enter zeros in the **Source MAC Address** field and set the **Source VID** field.

The following figure shows an example to limit bandwidth on all traffic from VLAN 3.

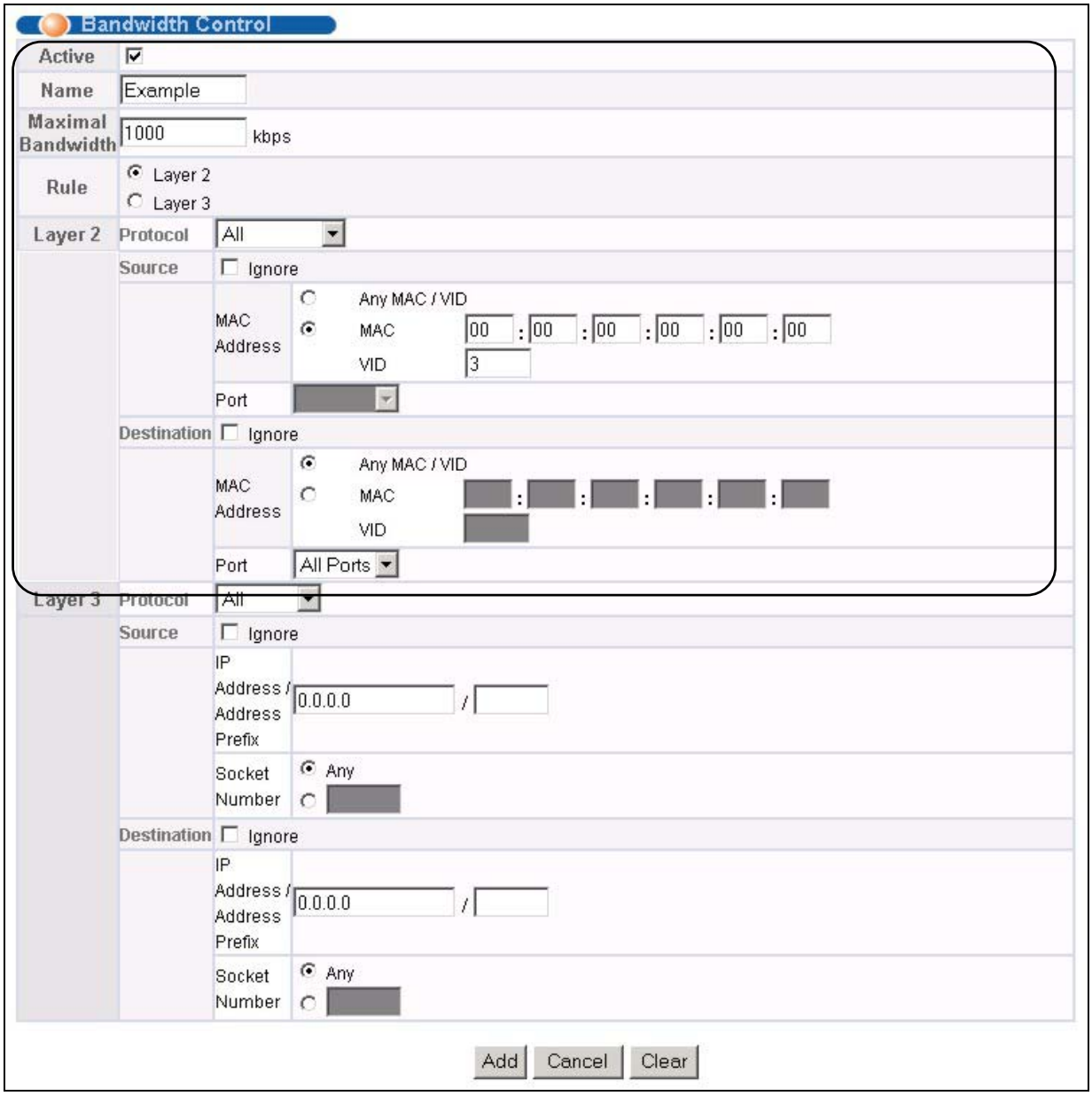


Figure 11-2 VLAN Bandwidth Control Example

11.2Viewing and Editing a Bandwidth Control Rule

To view a summary of the rule configuration, scroll down to the summary table at the bottom of the **Bandwidth Control** screen.

To change the settings of a rule, click a number in the **Index** field.

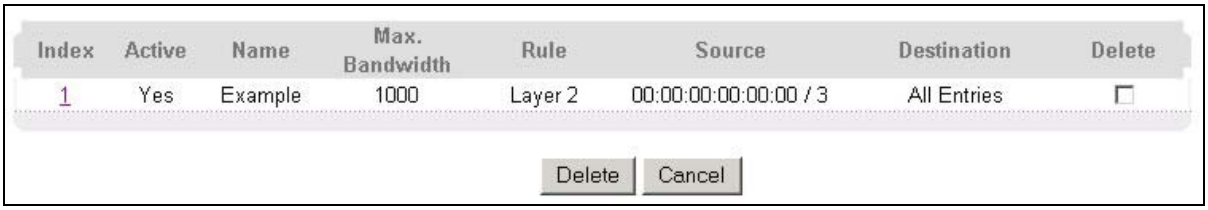


Figure 11-3 Bandwidth Control: Summary Table

The following table describes the labels in this screen.

Table 11-2 Bandwidth Control: Summary Table

LABEL	DESCRIPTION
Index	This field displays the index number of a bandwidth control rule. Click this number to edit the rule settings.
Active	This field indicates whether the bandwidth control rule is enabled (**Yes**) or disabled (**No**).
Name	This field displays the descriptive name of the rule.
Max. Bandwidth	This field displays the maximum bandwidth allowed in kilobits per second (kbps) for the rule.
Rule	This field displays the network layer (**Layer 2** or **Layer3**) to which this rule applies.
Source	For **Layer 2** rules, this field displays the source port number, the source MAC address with the VLAN identification number to which the MAC address belongs or a combination of the two. For **Layer 3** rules, this field displays the source protocol socket number, the source IP address and the number of ones in the subnet mask octet or a combination of the two. **All Entries** means all IP/MAC addresses from all ports.
Destination	For **Layer 2** rules, this field displays the destination protocol port number, the destination MAC address with the VLAN identification number to which the MAC address belongs or a combination of the two. For **Layer 3** rules, this field displays the destination protocol socket number, the destination IP address and the number of ones in the subnet mask octet or a combination of the two. **All Entries** means all IP/MAC addresses from all ports.
Delete	To delete a rule, select its checkbox in this column and then click the **Delete** button.
Add	To add a rule, click this button.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

Chapter 12
Broadcast Storm Control

This chapter introduces and shows you how to configure the broadcast storm control feature.

12.1 Introducing Broadcast Storm Control

Broadcast storm control limits the number of broadcast frames that can be stored in the switch buffer or sent out from the switch. Broadcast frames that arrive when the buffer is full are discarded. Enable this feature to reduce broadcast traffic coming into your network.

12.2 Configuring Broadcast Storm Control

Click **Advanced Application**, **Broadcast Strom Control** in the navigation panel to display the screen as shown next.

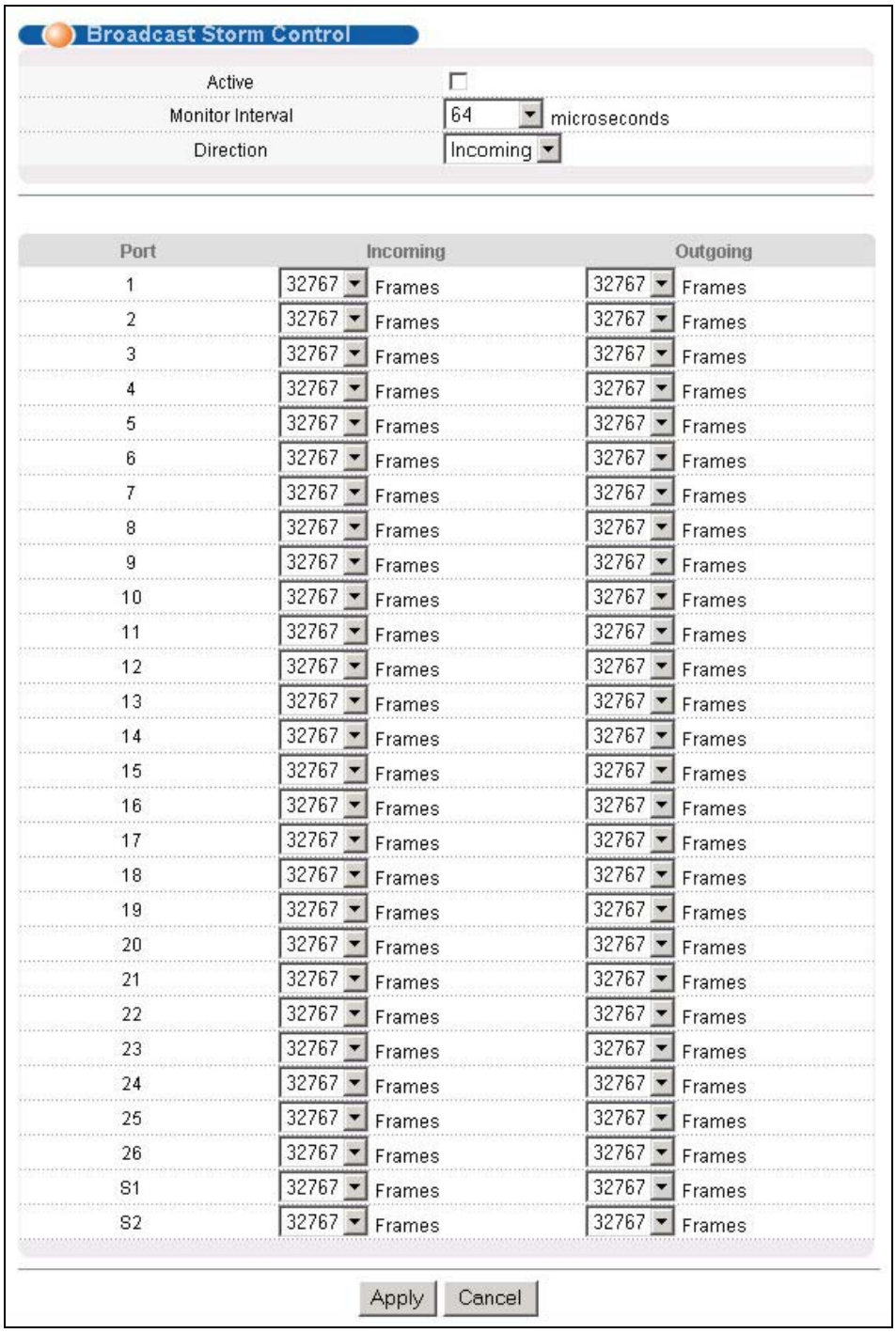


Figure 12-1 Broadcast Storm Control

The following table describes the labels in this screen.

Table 12-1 Broadcast Storm Control

LABEL	DESCRIPTION
Active	Select this check box to enable broadcast storm control. Clear this check box to disable the feature.

Table 12-1 Broadcast Storm Control

LABEL	DESCRIPTION
Monitor Interval	When the **Monitor Interval** time period expires, each port begins counting broadcast frames allowed in its buffers anew. Select a time period from **64**, **1024**, **8000**, **256000** microseconds.
Direction	Choose to monitor broadcast packets coming into the switch (**Incoming**) or going out of the switch (**Outgoing**).
Port	This field displays a port number.
Incoming	From the drop-down list box, select how many broadcast frames the port can store in the switch buffer.
Outgoing	From the drop-down list box, select how many frames the port will send out
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Chapter 13 Mirroring

This chapter discusses the Mirror setup screens.

13.1 Introduction to Port Mirroring

Port mirroring allows you to copy traffic going from one or all ports to another or all ports in order that you can examine the traffic from the mirror port (the port you copy the traffic to) without interference.

13.2 Port Mirroring Configuration

Click **Advanced Application**, **Mirroring** in the navigation panel to display the **Mirroring** screen.

13.2.1 Note About Configuration

The following rules apply when configuring mirroring.

- The rule applies to traffic flowing in both directions if both a source and destination are specified.
- The rule applies to traffic flowing in one direction if either a source or destination is specified.
- No any-to-any rules are allowed. That is, you cannot select **Ignore** for both the source and destination ports.
- No blank rules are allowed. If you do not select **Ignore**, you must set the related fields.

13.2.2 Setting Up the Mirror Port

You must first select a mirror port. A mirror port is a port that copies the traffic of other ports.

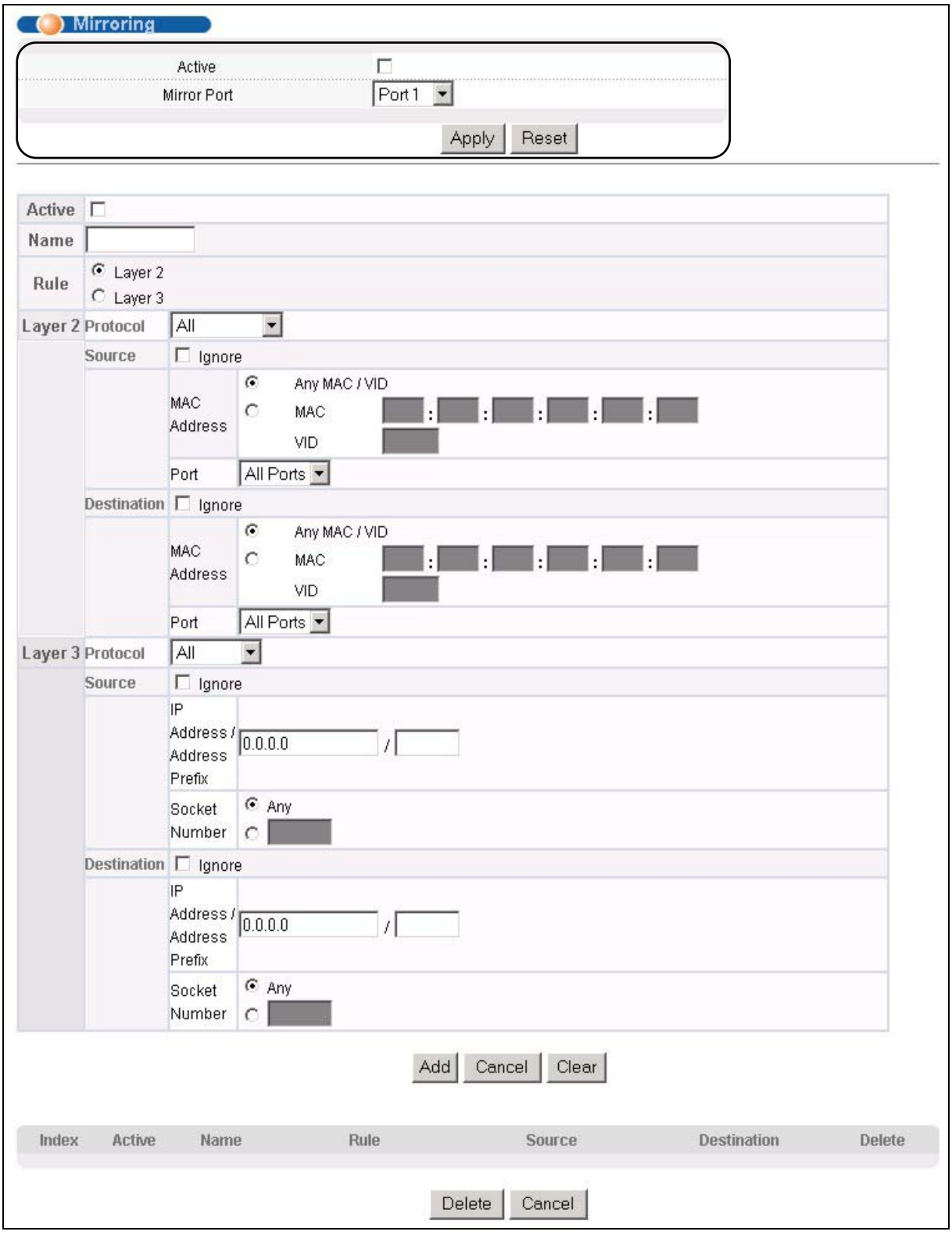


Figure 13-1 Mirroring: Mirror Port Setting

The following table describes the related labels in this screen.

Table 13-1 Mirroring: Mirror Port Setting

LABEL	DESCRIPTION
Active	Clear this check box to deactivate port mirroring on the switch.
Mirror Port	The mirror port is the port you copy the traffic to in order to examine it in more detail without interfering with the traffic flow on the original port(s). Select this port from this drop-down list box.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to start configuring the screen again.

13.2.3 Configuring a Mirroring Rule

After you select a mirror port, configure a mirroring rule in the related fields in the **Mirroring** screen.

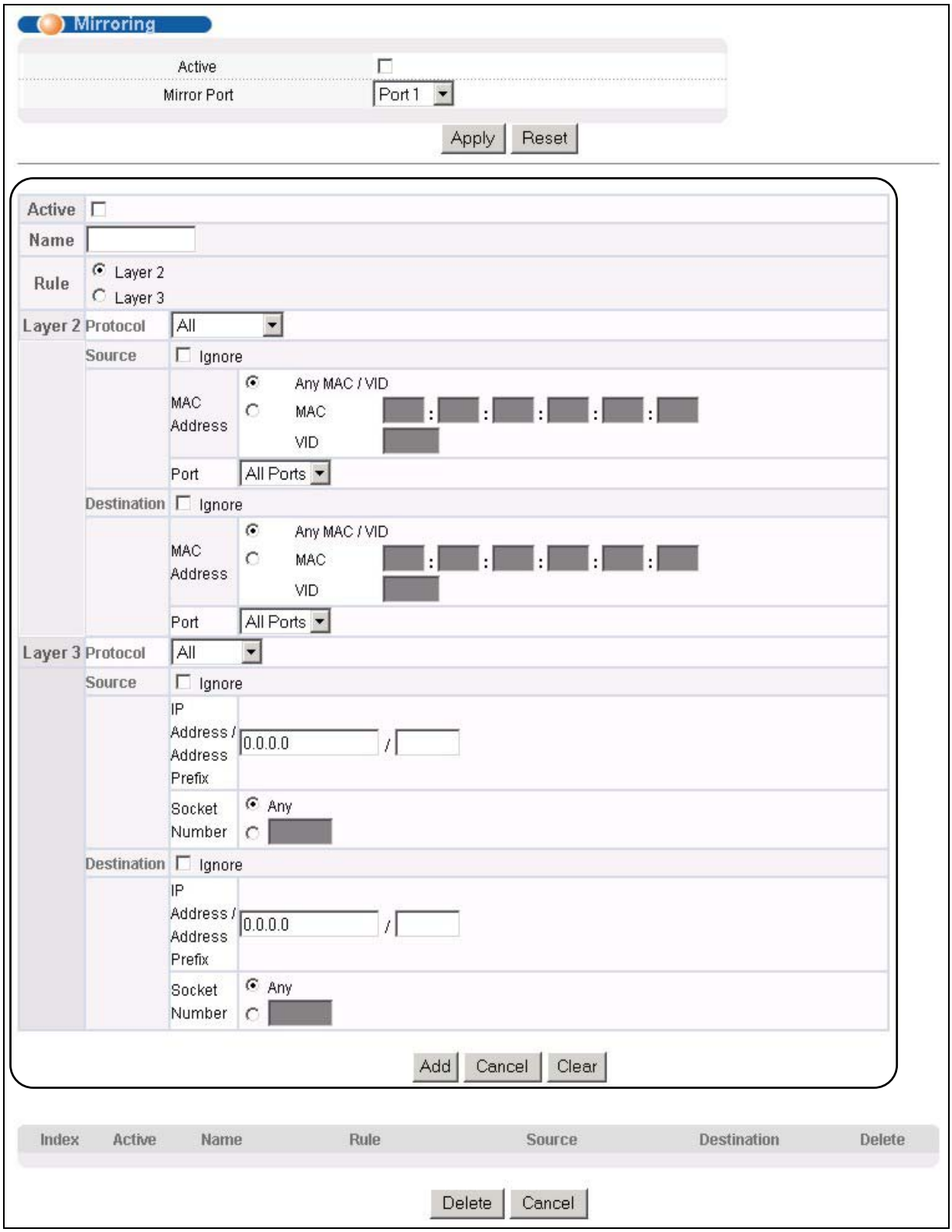


Figure 13-2 Mirroring: Configuration

The following table describes the related labels in this screen.

Table 13-2 Mirroring: Configuration

LABEL	DESCRIPTION
Active	Make sure to select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by deselecting this check box.
Name	Type a descriptive name for this rule. This is for identification purpose only.
Rule	Specify to which network layer (**Layer 2** or **Layer 3**) this rule applies.
Layer 2 Set the related fields when you select **Layer 2** in the **Rule** field.	
The VID for the source and destination must be the same.	
Protocol	Select the protocol traffic to which this rule applies.
Source	The next three fields pertain to the source MAC address and source port.
Ignore	Click this check box to ignore any traffic from all source ports.
MAC Address	Select **Any MAC/VID** to apply the rule to all MAC address and VLAN group identification numbers. To specify a source, select the second choice and type a MAC address in valid MAC address format (six hexadecimal character pairs) and then enter the VLAN group identification number.
Port	Select the port to which the rule should be applied. You may choose one port only or all ports (**All Ports**).
Destination	The next three fields pertain to the destination MAC address and destination port.
Ignore	Click this check box to ignore any traffic to all destination ports.
MAC Address	Select **Any MAC/VID** to apply the rule to all MAC address and VLAN group identification numbers. To specify a destination, select the second choice and type a MAC address in valid MAC address format (six hexadecimal character pairs) and then enter the VLAN group identification number.
Port	Select the port to which the rule should be applied. You may choose one port only or all ports (**All Ports**).
Layer 3 Set the related fields below when you select **Layer 3** in the **Rule** field.	
Protocol	Select the protocol traffic to which this rule applies.
Source	The next three fields pertain to the source IP address and source port.
Ignore	Click this check box to ignore any traffic from all source ports.
IP Address/Address Prefix	Enter a source IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask.

Table 13-2 Mirroring: Configuration

LABEL	DESCRIPTION
Socket Number	**You *must* set the** IP Address/Address Prefix **fields and select either** UDP **or** TCP **in the** Protocol **field before you can configure the socket number.**
	Select **Any** to apply to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number.
Destination	The next three fields pertain to the destination IP address and destination port.
Ignore	Click this check box to ignore any traffic to all destination ports.
IP Address/Address Prefix	Enter a destination IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask.
Socket Number	**You *must* set the** IP Address/Address Prefix **fields and select either** UDP **or** TCP **in the** Protocol **field before you can configure the socket number.**
	Select **Any** to apply to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number.
Add	Click **Add** to inset the entry to the summary table below.
Cancel	Click **Cancel** to reset the fields back to your previous configuration.
Clear	Click **Clear** to reset the fields back to the factory defaults.

13.2.4 Editing and Viewing a Mirroring Rule

To view a summary of the rule configuration, scroll down to the summary table at the bottom of the **Mirroring** screen.

To change the settings of a rule, click a number in the **Index** field.

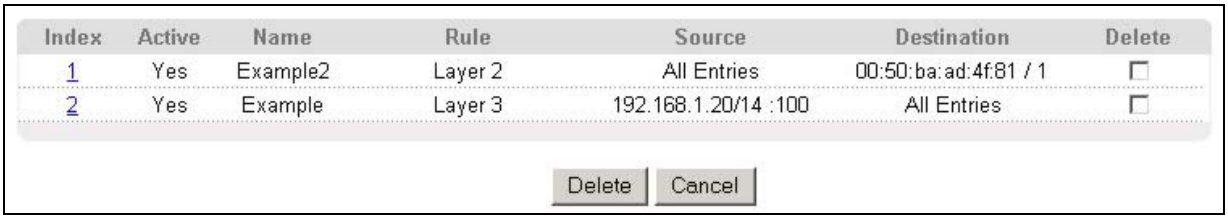


Figure 13-3 Mirroring: Summary Table

The following table describes the related labels in this screen.

Table 13-3 Mirroring: Summary Table

LABEL	DESCRIPTION
Index	This field displays the index number of a rule. Click this number to edit the rule settings.
Active	This field indicates whether the rule is enabled (**Yes**) or disabled (**No**).

Table 13-3 Mirroring: Summary Table

LABEL	DESCRIPTION
Name	This field displays the descriptive name of the rule.
Rule	This field displays the network layer (**Layer 2** or **Layer 3**) to which this rule applies.
Source	For **Layer 2** rules, this field displays the source port number, the source MAC address with the VLAN identification number to which the MAC address belongs or a combination of the two. For **Layer 3** rules, this field displays the source protocol socket number, the source IP address and the address prefix or a combination of the two. **All Entries** means all IP/MAC addresses from all ports.
Destination	For **Layer 2** rules, this field displays the destination port number, the destination MAC address with the VLAN identification number to which the MAC address belongs or a combination of the two. For **Layer 3** rules, this field displays the destination protocol socket number, the destination IP address and the address prefix or a combination of the two. **All Entries** means all IP/MAC addresses from all ports.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

Chapter 14
Link Aggregation

This chapter shows you how to logically aggregate physical links to form one logical, higher-bandwidth link.

14.1 Introduction to Link Aggregation

Link aggregation (trunking) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link.

However, the more ports you aggregate then the fewer available ports you have. A trunk group is one logical link containing multiple ports.

The beginning port of each trunk group must be physically connected to form a trunk group. Ports should be physically linked in consecutive order without gaps when forming trunk groups.

Table 14-1 Trunk Groups

TRUNK GROUP	BEGINNING PORT	PORT RANGE
1	1	1 to 8
2	9	9 to 16
3	17	17 to 24
4	25	25 and 26 (the uplink ports)
5	S1	S1 and S2 (the stacking ports)

14.1.1 Dynamic Link Aggregation

The ES-4024 adheres to the 802.3ad standard for static and dynamic (LACP) port trunking.

The ES-4024 supports the link aggregation IEEE802.3ad standard. This standard describes the Link Aggregate Control Protocol (LACP), which is a protocol that dynamically creates and manages trunk groups.

When you enable LACP link aggregation on a port, the port can automatically negotiate with the ports at the remote end of a link to establish trunk groups. LACP also allows port redundancy, that is, if an operational port fails, then one of the “standby” ports become operational without user intervention

Please note that:

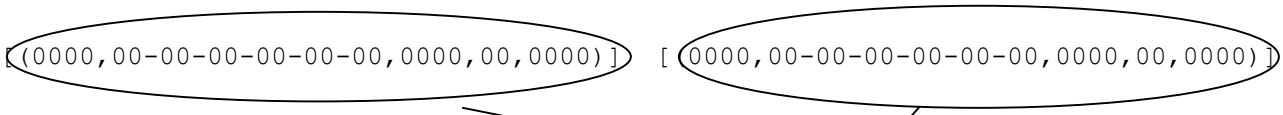
- You must connect all ports point-to-point to the same Ethernet switch and configure the ports for LACP trunking.
- LACP only works on full-duplex links.

- All ports in the same trunk group must have the same media type, speed, duplex mode and flow control settings.

Configure trunk groups or LACP before you connect the Ethernet switch to avoid causing network topology loops.

14.1.2 Link Aggregation ID

LACP aggregation ID consists of the following information:



Local switch				
0000	00-00-00-00-00	0000	00	0000
System priority	Local switch MAC address	Key	Port Priority[1]	Port Number[1]

Peer switch				
0000	00-00-00-00-00	0000	00	0000
System priority	MAC address	Key	Port Priority[1]	Port Number[1]

Figure 14-1 Link Aggregation ID

14.2 Link Aggregation Configuration

Click **Advanced Application**, **Link Aggregation** in the navigation panel. The **Link Aggregation Control Protocol Status screen** displays by default.

[1] This is "0" as it is the aggregator ID for the trunk group, not the individual port.

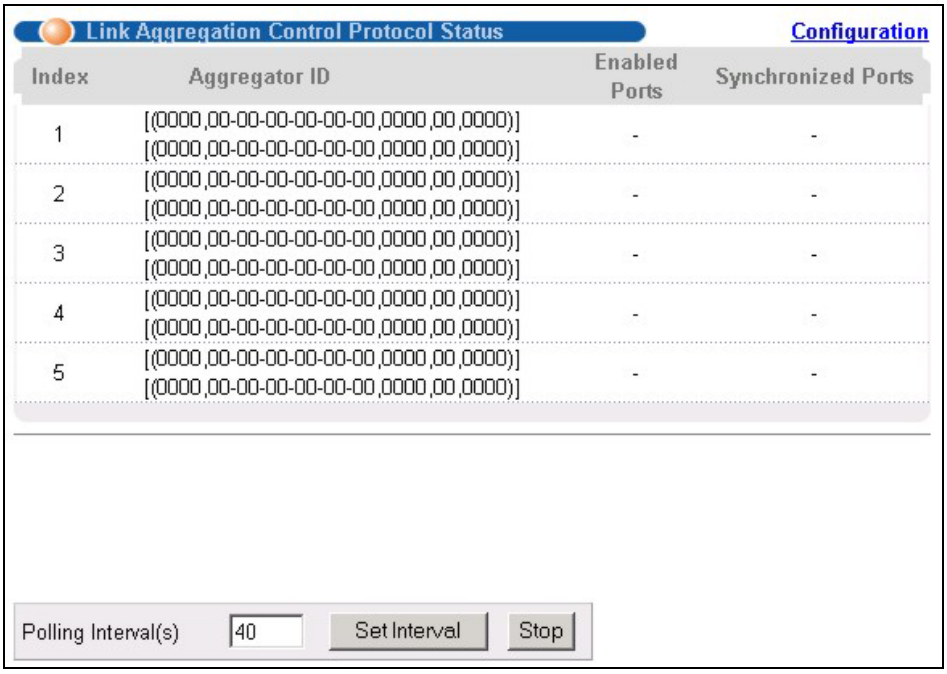


Figure 14-2 Link Aggregation Control Protocol Status

The following table describes the labels in this screen.

Table 14-2 Link Aggregation Control Protocol Status

LABEL	DESCRIPTION
Index	This field displays the trunk ID to identify a trunk group, that is, one logical link containing multiple ports.
Aggregator ID	Refer to *Figure 14-1* for more information on this field.
Enabled Port	These are the ports you have configured in the **Link Aggregation** screen to be in the trunk group.
Synchronized Ports	These are the ports that are currently transmitting data as one logical link in this trunk group.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt statistic polling.

14.3Link Aggregation Setup

Click **Configuration** in the **Link Aggregation Control Protocol Status** screen to display the screen shown next.

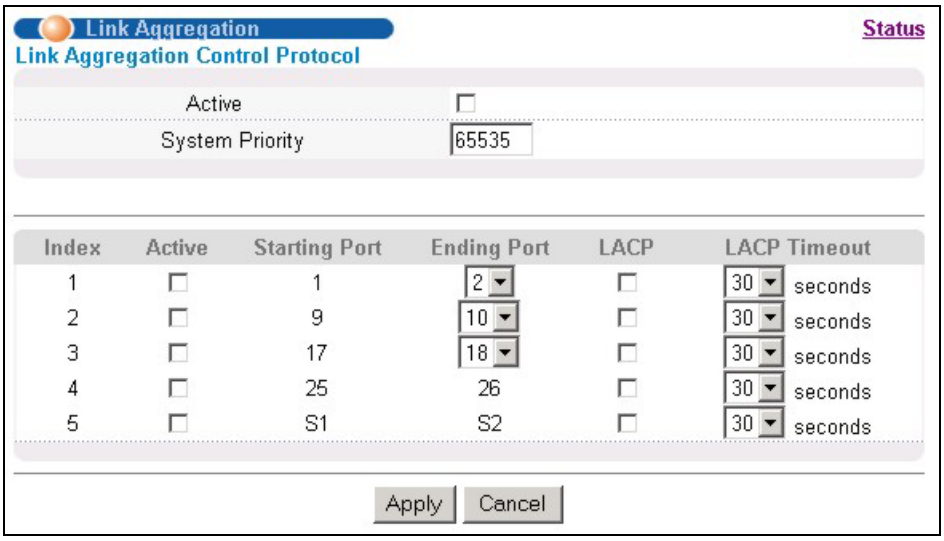


Figure 14-3 Link Aggregation: Configuration

The following table describes the labels in this screen.

Table 14-3 Link Aggregation: Configuration

LABEL	DESCRIPTION
Link Aggregation Control Protocol	
Active	Select this checkbox to enable Link Aggregation Control Protocol (LACP).
System Priority	LACP system priority is a number between 1 and 65,355. The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP “server”. The LACP “server” controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregate Control Protocol (LACP). The smaller the number, the higher the priority level.
Index	The index identifies the trunk group, that is, one logical link containing multiple ports
Active	Make sure to select this check box to activate the trunk group. You may temporarily deactivate a trunk group without deleting it by clearing this check box.
Starting Port	This is the beginning port in the trunk group’s port range and is not configurable (see *Table 14-1*).
Ending Port	Select the end port in the port range from the drop-down list box if applicable (see *Table 14-1*).
LACP	Select this check box to enable LACP for a trunk.
LACP Timeout	Timeout is the time interval between the individual port exchanges of LACP packets in order to check that the peer port in the trunk group is still up. If a port does not respond after three tries, then it is deemed to be “down” and is removed from the trunk. Set a short timeout (one second) for busy trunked links to ensure that disabled ports are removed from the trunk group as soon as possible. Select either 1 second or 30 seconds.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Chapter 15
Port Authentication

This chapter describes the 802.1x authentication method and RADIUS server connection setup.

15.1 Introduction to Authentication

IEEE 802.1x is an extended authentication protocol[2] that allows support of RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting[3] management on a network RADIUS server.

15.1.1 RADIUS

RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS authentication allows you to validate an unlimited number of users from a central location.

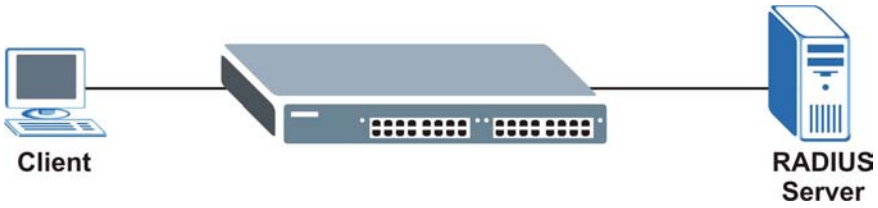


Figure 15-1 RADIUS Server

15.2 Configuring Port Authentication

To enable port authentication, first activate IEEE802.1x security (both on the ES-4024 and the port(s)) then configure the RADIUS server settings.

Click **Advanced Application**, **Port Authentication** in the navigation panel to display the screen as shown.

[2] At the time of writing, only Windows XP of the Microsoft operating systems supports it. See the Microsoft web site for information on other Windows operating system support. For other operating systems, see its documentation. If your operating system does not support 802.1x, then you may need to install 802.1x client software.

[3] Not available at the time of writing.

Figure 15-2 Port Authentication

15.2.1 Activating IEEE802.1x Security

From the **Port Authentication** screen, display the configuration screen as shown.

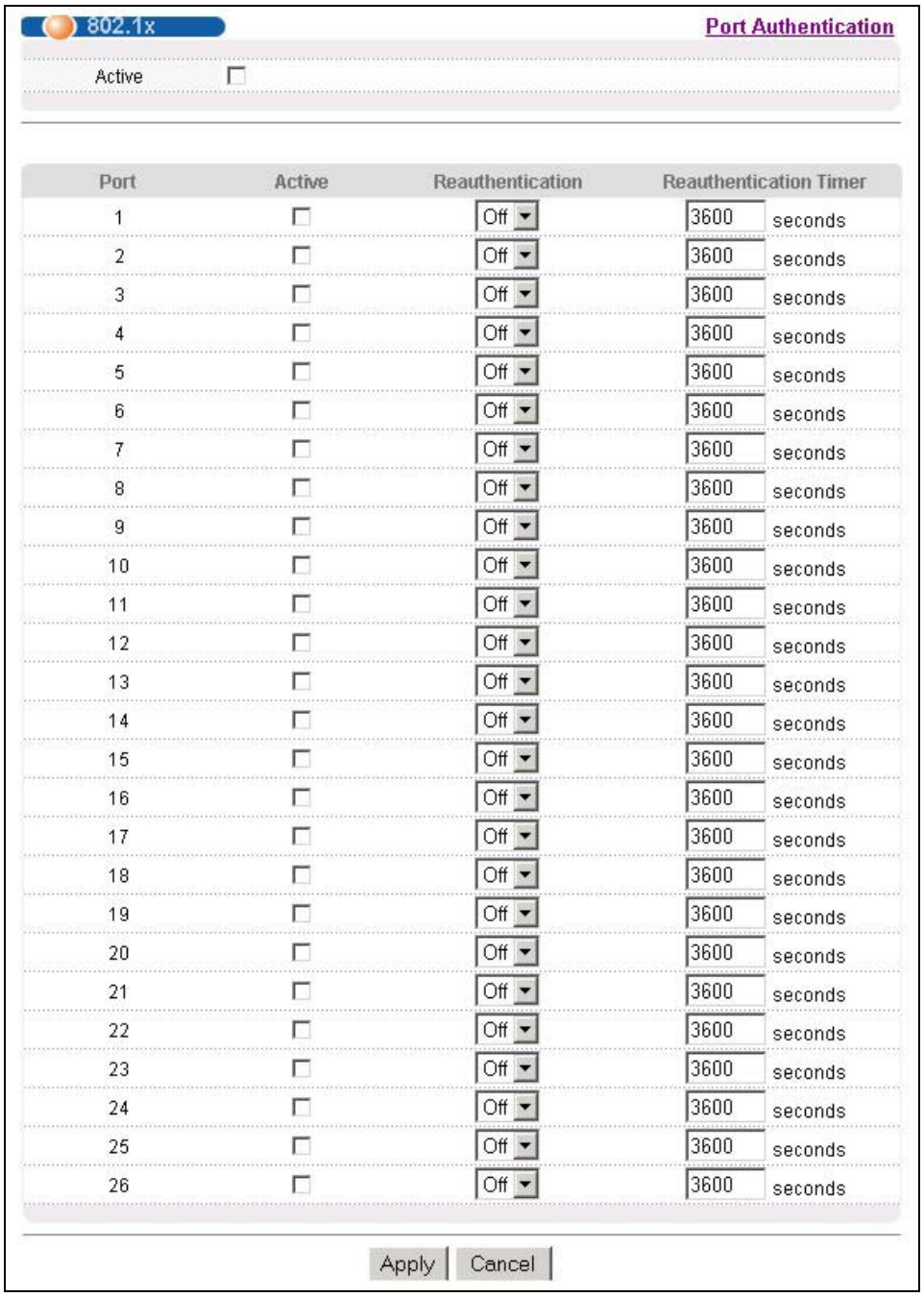


Figure 15-3 Port Authentication: 802.1x

The following table describes the labels in this screen.

Table 15-1 Port Authentication: 802.1x

LABEL	DESCRIPTION
Active	Select this check box to permit 802.1x authentication on the switch.
	You must first enable 802.1x authentication on the switch before configuring it on each port.

Table 15-1 Port Authentication: 802.1x

LABEL	DESCRIPTION
Port	This field displays a port number.
Active	Select this checkbox to permit 802.1x authentication on this port. You must first allow 802.1x authentication on the switch before configuring it on each port.
Reauthentication	Specify if a subscriber has to periodically re-enter his or her username and password to stay connected to the port.
Reauthentication Timer	Specify how often a client has to re-enter his or her username and password to stay connected to the port.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

15.2.2 Configuring RADIUS Server Settings

From the **Port Authentication** screen, display the configuration screen as shown.

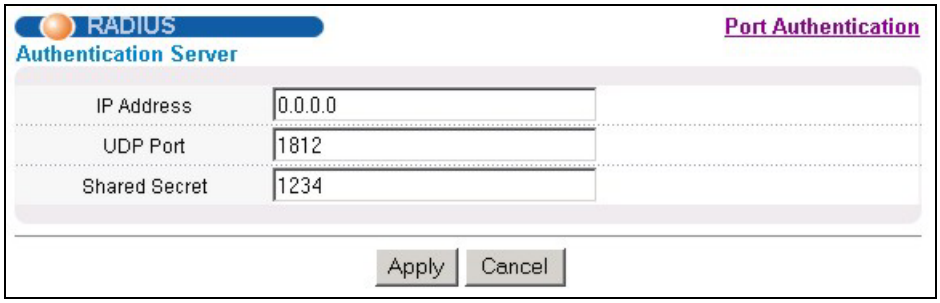


Figure 15-4 Port Authentication: RADIUS

The following table describes the labels in this screen.

Table 15-2 Port Authentication: RADIUS

LABEL	DESCRIPTION
Authentication Server	
IP Address	Enter the IP address of the external RADIUS server in dotted decimal notation.
UDP Port	The default port of the RADIUS server for authentication is **1812**. You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 30 alphanumeric characters) as the key to be shared between the external RADIUS server and the switch. This key is not sent over the network. This key must be the same on the external RADIUS server and the switch.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Chapter 16
Port Security

This chapter shows you how to set up port security.

16.1 About Port Security

Port security allows only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on the switch. The switch can learn up to 16K MAC addresses in total with no limit on individual ports other than the sum cannot exceed 16K.

For maximum port security, enable this feature, disable Mac address learning and configure static MAC address(es) for a port. It is not recommended you disable **Port Security** together with MAC address learning as this will result in many broadcasts.

16.2 Port Security Setup

Click **Advanced Application**, **Port Security** in the navigation panel to display the screen as shown.

Figure 16-1 Port Security

The following table describes the labels in this screen.

Table 16-1 Port Security

LABEL	DESCRIPTION
Port	This field displays a port number.
Active	Select this check box to enable MAC address learning on this port.
Address Learning	MAC address learning reduces outgoing broadcast traffic. For MAC address learning to occur on a port, the port itself must be active with address learning enabled.

Table 16-1 Port Security

LABEL	DESCRIPTION
Limited Number of Learned MAC Address	Use this field to limit the number of (dynamic) MAC addresses that may be learned on a port. For example, if you set this field to "5" on port 2, then only the devices with these five learned MAC addresses may access port 2 at any one time. A sixth device would have to wait until one of the five learned MAC addresses aged out. MAC address aging out time can be set in the **Switch Setup** screen. The valid range is from “0” to “254”. “0” means this feature is disabled, so the switch will learn MAC addresses up to the global limit of 16K.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Chapter 17 DHCP

This chapter shows you how to configure the DHCP feature.

17.1 About DHCP

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual computers to obtain TCP/IP configuration at start-up from a server. You can configure the ES-4024 as a DHCP server or disable it. When configured as a server, the ES-4024 provides the TCP/IP configuration for the clients. If you disable the DHCP service, you must have another DHCP server on your LAN, or else the computer must be manually configured.

17.1.1 DHCP modes

The ES-4024 can be configured as a DHCP server or DHCP relay agent.

- If you configure the ES-4024 as a DHCP server, it will maintain the pool of addresses and distribute them to your LAN computers.
- If there is an Ethernet device that performs the DHCP server function for your network, then you can configure the ES-4024 as a DHCP relay agent. When the ES-4024 receives a request from a computer on your network, it contacts the Ethernet device (the DHCP server) for the necessary IP information, and then relays the assigned information back to the computer.

17.2 Configuring DHCP

Click **Advanced Application**, **DHCP** in the navigation panel to display the screen as shown next.

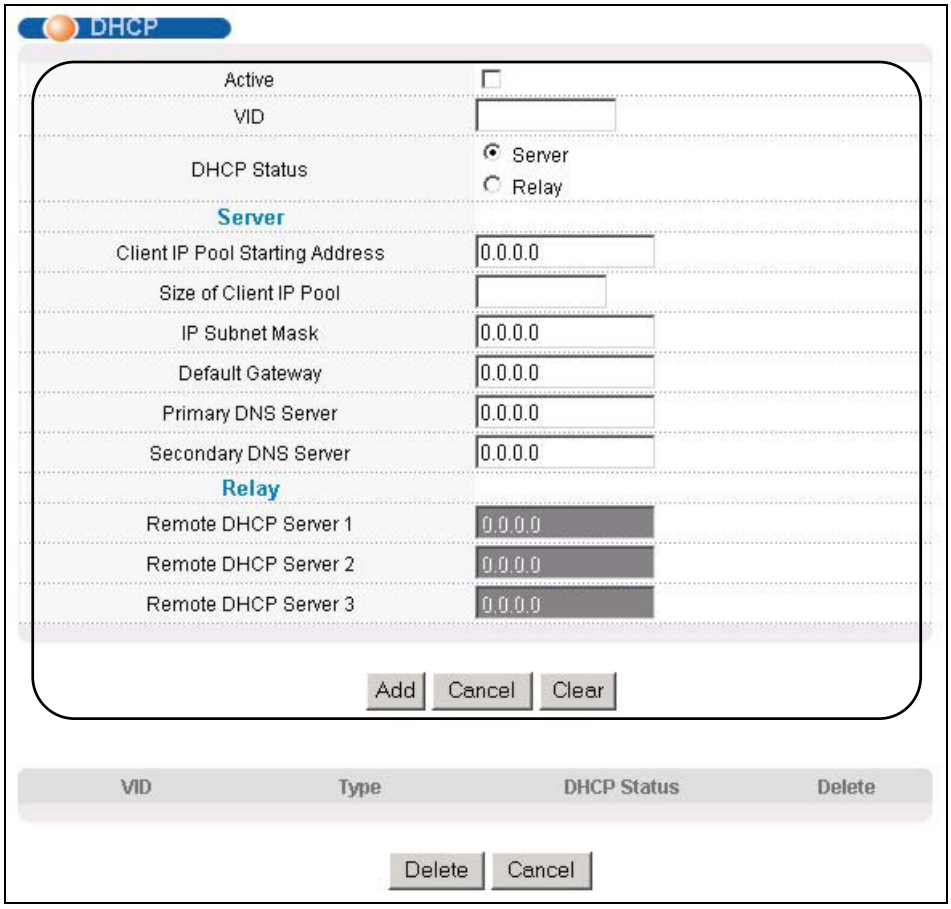


Figure 17-1 DHCP

The following table describes the labels in this screen.

Table 17-1 DHCP

LABEL	DESCRIPTION
Active	Select this check box to enable the DHCP settings.
VID	Enter the ID number of the VLAN group to which this DHCP settings apply.
DHCP Status	Select **Sever** to set the ES-4024 to act as a DHCP server. Select **Relay** to set the ES-4024 to act as a DHCP relay. Then set the corresponding fields below.
Server The fields are editable when you select **Server** in the **DHCP Status** field.	
Client IP Pool Starting Address	Specify the first of the contiguous addresses in the IP address pool.
Size of Client IP Pool	Specify the size, or count of the IP address pool.
IP Subnet Mask	Enter the subnet mask of the DHCP Server.
Default Gateway	Enter the IP address of the default gateway device.

Table 17-1 DHCP

LABEL	DESCRIPTION
Primary/ Secondary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Relay The fields are editable when you select **Relay** in the **DHCP Status** field.	
Remote DHCP Server 1.. 3	Enter the IP address(es) of the DHCP server(s).
Add	Click **Add** to insert the settings as a new entry in the summary table.
Cancel	Click **Cancel** to reset the fields to your previous configurations.
Clear	Click **Clear** to reset the fields back to the factory defaults.

17.3Viewing and Editing DHCP Settings

To view a summary of the DHCP settings, scroll down to the summary table at the bottom of the **DHCP** screen.

To change the settings of a rule, click a number in the **Index** field.

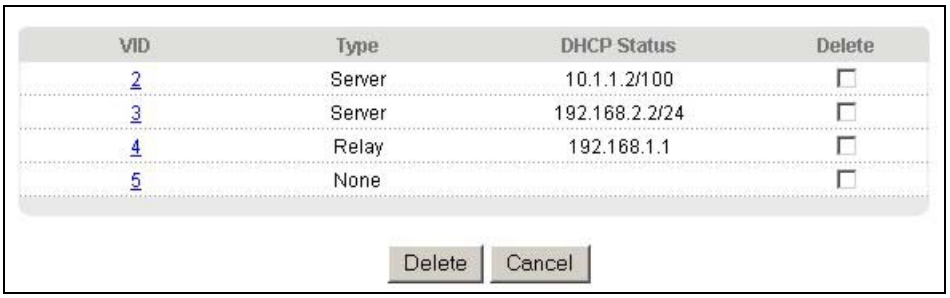


Figure 17-2 DHCP: Summary Table

The following table describes the labels in the summary table.

Table 17-2 DHCP: Summary Table

LABEL	DESCRIPTION
VID	This field displays the ID number of the VLAN group to which this DHCP settings apply.
Type	This field displays the type of the DHCP mode (**Server** or **Relay**) for this entry. **None** indicates the rule is inactive.
DHCP Status	This field displays the client IP pool starting address and the size of client IP pool if the **Type** field displays **Server**. This field displays the IP address of a DHCP server if the **Type** field is **Relay**.
Delete	Click **Delete** to remove the selected entry.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

Chapter 18 Access Control

This chapter describes how to control access to the switch.

18.1 Access Control Overview

1. A console port access control session and Telnet access control session cannot coexist. The console port has higher priority. If you telnet to the switch and someone is already logged in from the console port, then you will see the following message.

```
"Local administrator is configuring this device now!!!
Connection to host lost."
```

Figure 18-1 Console Port Priority

2. A console port or Telnet session can coexist with one FTP session, up to five Web sessions (five different usernames and passwords) and/or limitless SNMP access control sessions.

Table 18-1 Access Control Summary

	Console port	Telnet	FTP	Web	SNMP
Number of sessions allowed	1	1	1	5	No limit
Number of concurrent sessions allowed	1 console port or Telnet. Console port has priority.		1	5	No limit

18.2 The Access Control Main Screen

Click **Advanced Application**, **Access Control** in the navigation panel to display the main screen as shown.

Figure 18-2 Access Control

18.3 About SNMP

Simple Network Management Protocol (SNMP) is an application layer protocol used to manage and monitor TCP/IP-based devices. SNMP is used to exchange management information between the network management system (NMS) and a network element (NE). A manager station can manage and monitor the ES-4024 through the network via SNMP version one (SNMPv1) and/or SNMP version 2c. The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

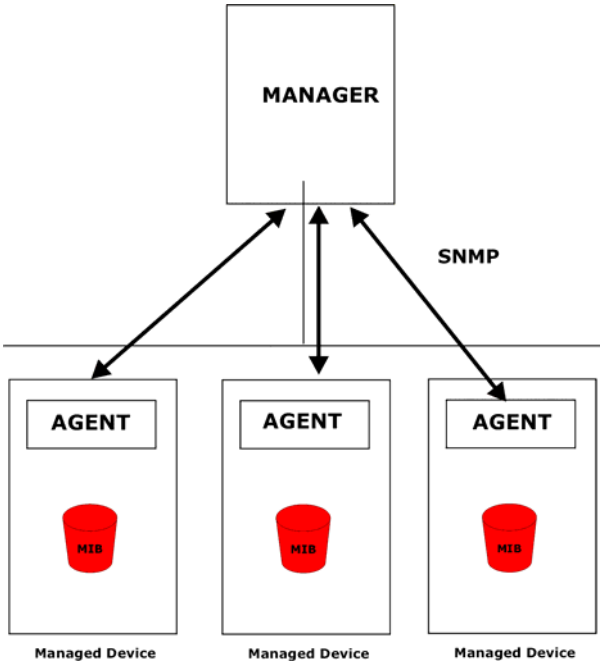


Figure 18-3 SNMP Management Model

An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed switch (the ES-4024). An agent translates the local management information from the managed switch into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a switch. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

Table 18-2 SNMP Commands

COMMAND	DESCRIPTION
Get	Allows the manager to retrieve an object variable from the agent.

Table 18-2 SNMP Commands

COMMAND	DESCRIPTION
GetNext	Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
Set	Allows the manager to set values for object variables within an agent.
Trap	Used by the agent to inform the manager of some events.

18.3.1 Supported MIBs

MIBs let administrators collect statistics and monitor status and performance.

The ES-4024 supports the following MIBs:

- SNMP MIB II (RFC 1213)
- RFC 1493 Bridge MIBs
- RFC 1155 SMI
- RFC 1757 RMON
- RFC 1157 SNMP v1
- RFC 1643 Ethernet MIBs
- RFC 2674 SNMPv2, SNMPv2c
- SNMPv2, SNMPv2c or later version, compliant with RFC 2011 SNMPv2 MIB for IP, RFC 2012 SNMPv2 MIB for TCP, RFC 2013 SNMPv2 MIB for UDP

18.3.2 SNMP Traps

The ES-4024 sends traps to an SNMP manager when an event occurs. SNMP traps supported are outlined in the following table.

Table 18-3 SNMP Traps

GENERIC TRAP	SPECIFIC TRAP	DESCRIPTION
0 (Cold Start)	0	This trap is sent when the ES-4024 is turned on.
1 (WarmStart)	0	This trap is sent when the ES-4024 restarts.
2 (linkDown)	0	This trap is sent when the Ethernet link is down.
3 (linkUp)	0	This trap is sent when the Ethernet link is up.
4 (authenticationFailure)	0	This trap is sent when an SNMP request comes from non-authenticated hosts.

18.3.3 Configuring SNMP

From the **Access Control** screen, display the **SNMP** screen. You can click **Access Control** to go back to the **Access Control** screen.

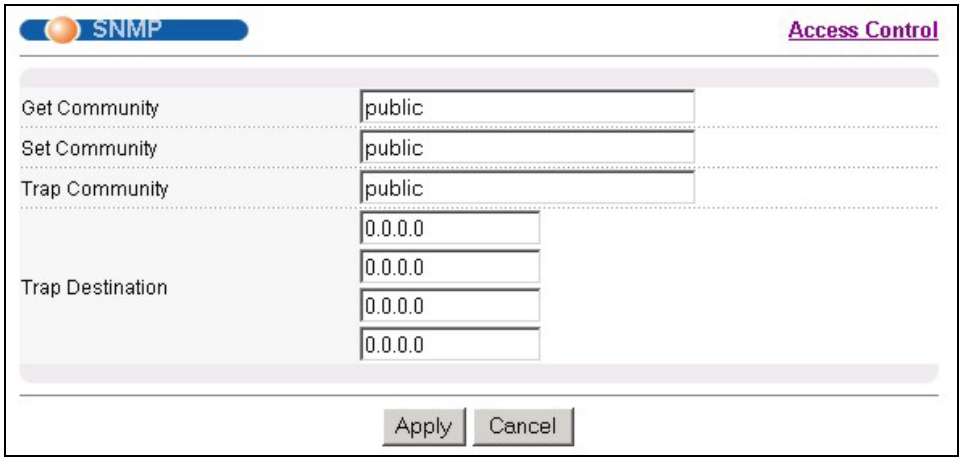


Figure 18-4 Access Control: SNMP

The following table describes the labels in this screen.

Table 18-4 Access Control: SNMP

LABEL	DESCRIPTION
Get Community	Enter the get community, which is the password for the incoming Get- and GetNext- requests from the management station.
Set Community	Enter the set community, which is the password for incoming Set- requests from the management station.
Trap Community	Enter the trap community, which is the password sent with each trap to the SNMP manager.
Trap Destination	Enter the IP addresses of up to four stations to send your SNMP traps to.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

18.3.4 Setting Up Login Accounts

Up to five people (one administrator and four non-administrators) may access the switch via web configurator at any one time.

1. An administrator is someone who can both view and configure switch changes. The username for the Administrator is always **admin**. The default administrator password is **1234**.

It is highly recommended that you change the default administrator password ("1234").

2. A non-administrator (username is something other than **admin**) is someone who can view but not configure switch changes.

Click **Access Control** from the navigation panel and then click **Logins** from this screen.

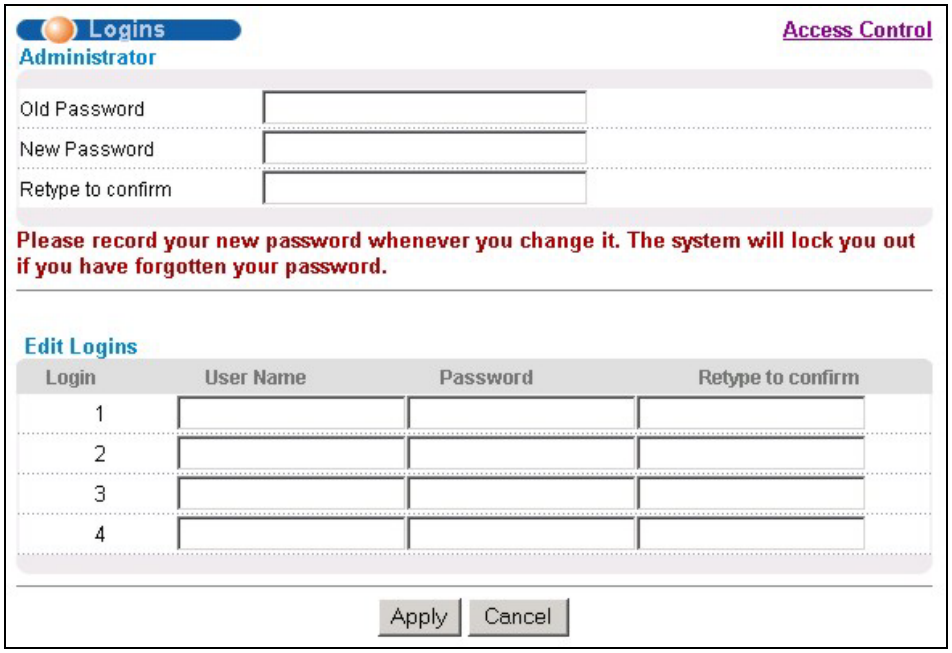


Figure 18-5 Access Control: Logins

The following table describes the labels in this screen.

Table 18-5 Access Control: Logins

LABEL	DESCRIPTION
Administrator This is the default administrator account with the “admin” user name. You cannot change the default administrator user name. Only the administrator has read/write access.	
Old Password	Type the existing system password ("1234" is the default password when shipped).
New Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation
Edit Logins You may configure passwords for up to four users. These people have read-only access.	
User Name	Set a user name (up to 30 characters long).
Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

18.4 Service Access Control

Service Access Control allows you to decide what services you may use to access the ES-4024. You may also change the default service port and configure "trusted computer(s)" for each service in the **Remote Management** screen (discussed later). Click **Access Control** to go back to the **Access Control** screen.

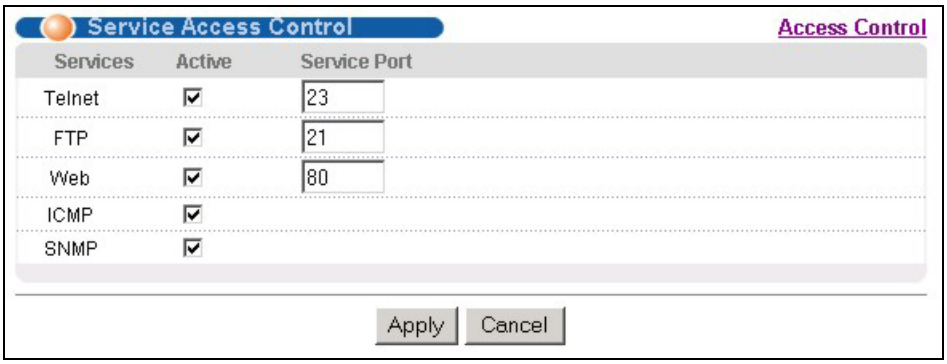


Figure 18-6 Access Control: Service Access Control

The following table describes the fields in this screen.

Table 18-6 Access Control: Service Access Control

LABEL	DESCRIPTION
Services	Services you may use to access the ES-4024 are listed here.
Active	Select this option for the corresponding services that you want to allow to access the ES-4024.
Service Port	For Telnet, FTP or web services, you may change the default service port by typing the new port number in the **Service Port** field. If you change the default port number then you will have to let people (who wish to use the service) know the new port number for that service.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

18.5 Remote Management

From the **Access Control** screen, display the **Remote Management** screen as shown next.

You can specify a group of one or more "trusted computers" from which an administrator may use a service to manage the switch. Click **Access Control** to return to the **Access Control** screen.

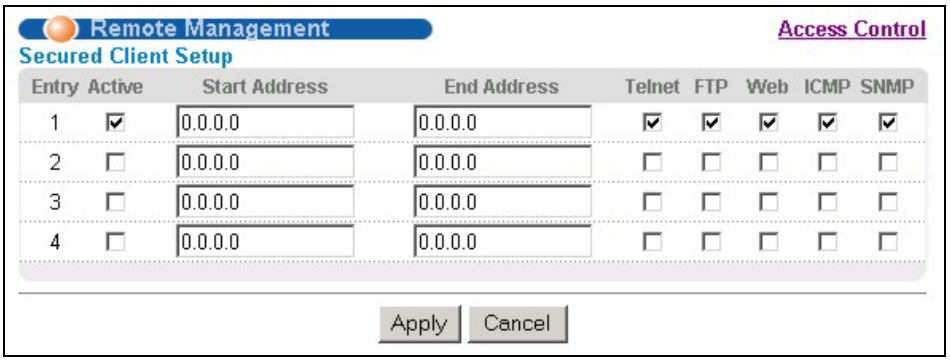


Figure 18-7 Access Control: Remote Management

The following table describes the labels in this screen.

Table 18-7 Access Control: Remote Management

LABEL	DESCRIPTION
Entry	This is the client set index number. A “client set” is a group of one or more “trusted computers” from which an administrator may use a service to manage the switch.
Active	Select this check box to activate this secured client set. Clear the check box if you wish to temporarily disable the set without deleting it.
Start Address End Address	Configure the IP address range of trusted computers from which you can manage this switch. The switch checks if the client IP address of a computer requesting a service or protocol matches the range set here. The switch immediately disconnects the session if it does not match.
Telnet/FTP/Web/ICMP/SNMP	Select services that may be used for managing the switch from the specified trusted computers.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Chapter 19 Differentiated Services

This chapter shows you how to configure Differentiated Services (DiffServ) on the ES.

19.1 Introduction to DiffServ

Quality of Service (QoS) mechanisms provide the best service on a per-flow guarantee. To fine-tune the levels of services on the priority of the traffic flow using QoS places a heavy burden on the network infrastructure.

DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

19.1.1 DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (ToS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

Figure 19-1 DiffServ: Differentiated Service Field

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

19.1.2 DiffServ Network Example

The following figure depicts a simple DiffServ network consisting of a group of contiguous DiffServ-compliant network devices.

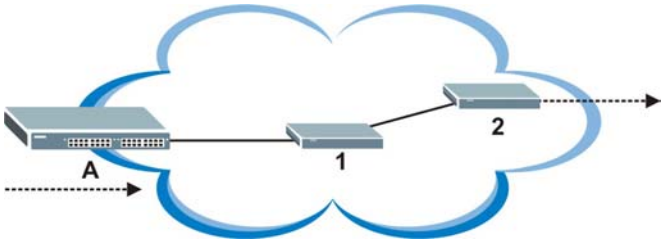


Figure 19-2 DiffServ Network Example

Switch A marks traffic flowing into the network based on the configured marking rules. Intermediary network devices 1 and 2 allocate network resources (such as bandwidth) by mapping the DSCP values and the associated policies.

19.2 Activating DiffServ

Activate DiffServ to allow the ES to enable DiffServ and apply marking rules and IEEE802.1p priority mapping on the selected port(s).

Click **Advanced Applications**, **DiffServ** in the navigation panel to display the screen as shown.

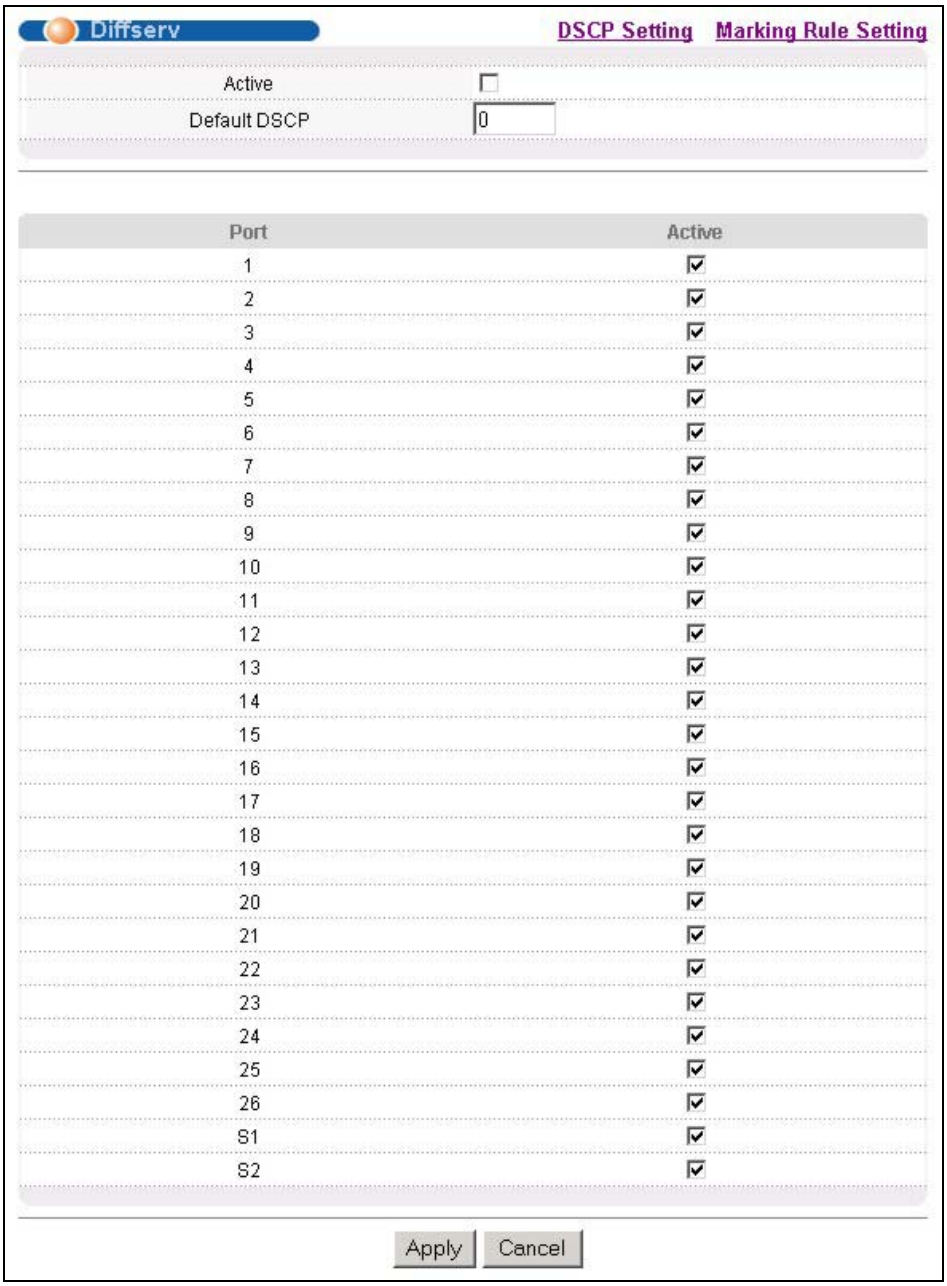


Figure 19-3 Advanced Applications: DiffServ

The following table describes the labels in this screen.

Table 19-1 Advanced Applications: DiffServ

LABEL	DESCRIPTION
Active	Select this option to enable DiffServ on the switch.
Default DSCP	Enter the default DSCP value (between 0 to 63) to use if no marking rule is configured for a traffic type.
Port	This field displays the index number of a port on the ES.
Active	Select this option to apply the default DSCP value you set in the **Default DSCP** field on a port.

Table 19-1 Advanced Applications: DiffServ

LABEL	DESCRIPTION
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to start configuring this screen again.

19.3 Configuring Marking Rules

Create DiffServ marking rules to set the DSCP values in the packets for the traffic flows.

19.3.1 Note About Configuration

The following rules apply when configuring DiffServ rules.

- The rule applies to traffic flowing in both directions if both a source and destination are specified.
- The rule applies to traffic flowing in one direction if either a source or destination is specified.
- No any-to-any rules are allowed. That is, you cannot select **Ignore** for both the source and destination ports.
- No blank rules are allowed. If you do not select **Ignore**, you must set the related fields.

In the **DiffServ** screen, click the **Making Rule Setting** link to display the screen as shown next.

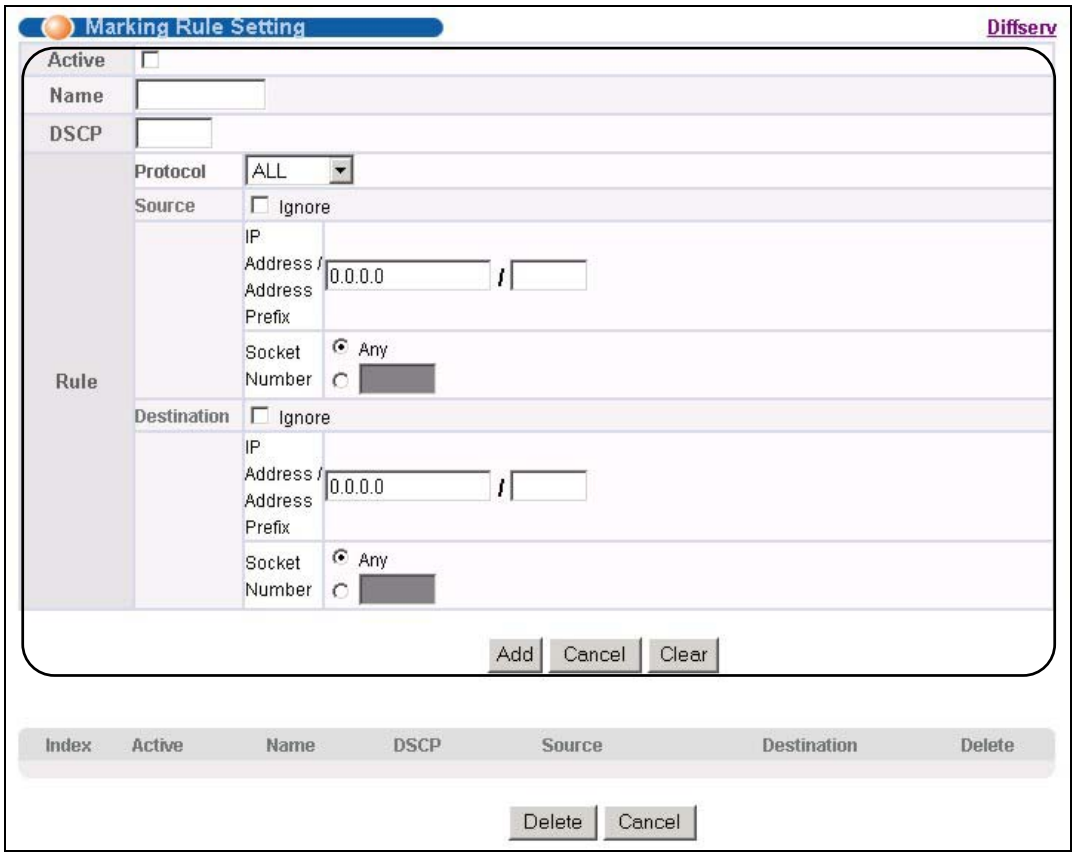


Figure 19-4 DiffServ: Marking Rule Setting

The following table describes the labels in this screen.

Table 19-2 DiffServ: Marking Rule Setting

LABEL	DESCRIPTION
Active	Select this option to enable this rule.
Name	Enter a description name for identification purposes.
DSCP	Enter a DSCP value (between 1 and 63) for this rule.
Rule	
Protocol	Select the application type to which this rule applies.
Source	Set the fields to configure the source of the traffic flow to which this rule applies.
Ignore	Click this check box to ignore any traffic from all source ports.
IP Address/Address Prefix	Enter a source IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask.
Socket Number	**You *must* set the** IP Address/Address Prefix **fields and select either** UDP **or** TCP **in the** Protocol **field before you can configure the socket number.** Specify the protocol port number to which the rule applies. Select **Any** to apply to all ports or select the second option and enter a port number.
Destination	Set the fields to configure the destination of the traffic flow to which this rule applies.
Ignore	Click this check box to ignore any traffic to all destination ports.
IP Address/Address Prefix	Enter a destination IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask.
Socket Number	**You *must* set the** IP Address/Address Prefix **fields and select either** UDP **or** TCP **in the** Protocol **field before you can configure the socket number.** Specify the protocol port number to which the rule should be applied. Select **Any** to apply to all ports or select the second option and enter a port number.
Add	Click **Add** to inset the entry to the summary table below.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Clear	Click **Clear** to reset the fields back to the factory defaults.

19.3.2 Viewing Marking Rule Summary

To view a summary of the marking rule configuration, scroll down to the bottom of the **Making Rule Setting** screen.

To change the settings of a rule, click a number in the **Index** field.

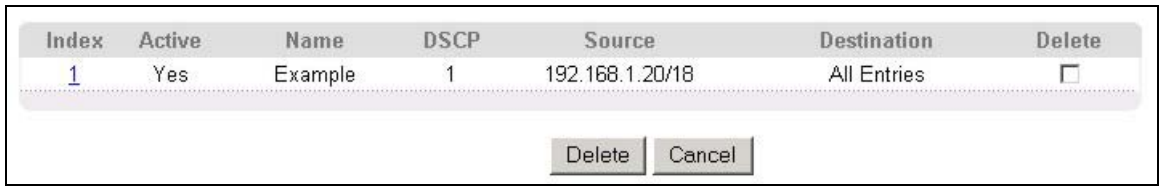


Figure 19-5 DiffServ: Marking Rule Summary

The following table describes the labels in the summary table.

Table 19-3 DiffServ: Marking Rule Summary

LABEL	DESCRIPTION
Index	This field displays the index number of the rule. Click an index number to edit the rule.
Active	This field displays **Yes** when the rule is enabled and **No** when is it disabled.
Name	This field displays the descriptive name for this rule. This is for identification purpose only.
DSCP	This field displays the DSCP value for this rule.
Source	This field displays the source protocol socket number, the source IP address and/or the address prefix. **All Entries** means all IP addresses from all ports.
Destination	This field displays the destination protocol socket number, the destination IP address and/or the address prefix. **All Entries** means all IP addresses from all ports.
Delete	Click **Delete** to remove the selected entry.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

19.4 DSCP-to-IEEE802.1p Priority Mapping

You can configure the DSCP to IEEE802.1p mapping to allow the ES to prioritize all traffic based on the incoming DSCP value according to the DiffServ to IEEE802.1p mapping table.

The following table shows the default DSCP-to-IEEE802.1P mapping.

Table 19-4 Default DSCP-IEEE802.1p Mapping

DSCP VALUE	0 – 7	8 – 15	16 – 23	24 – 31	32 – 39	40 – 47	48 – 55	56 – 63
IEEE802.1P	0	1	2	3	4	5	6	7

19.4.1 Configuring DSCP Settings

To change the DSCP-IEEE 802.1p mapping, click the **DSCP Setting** link in the **DiffServ** screen to display the screen as shown next.

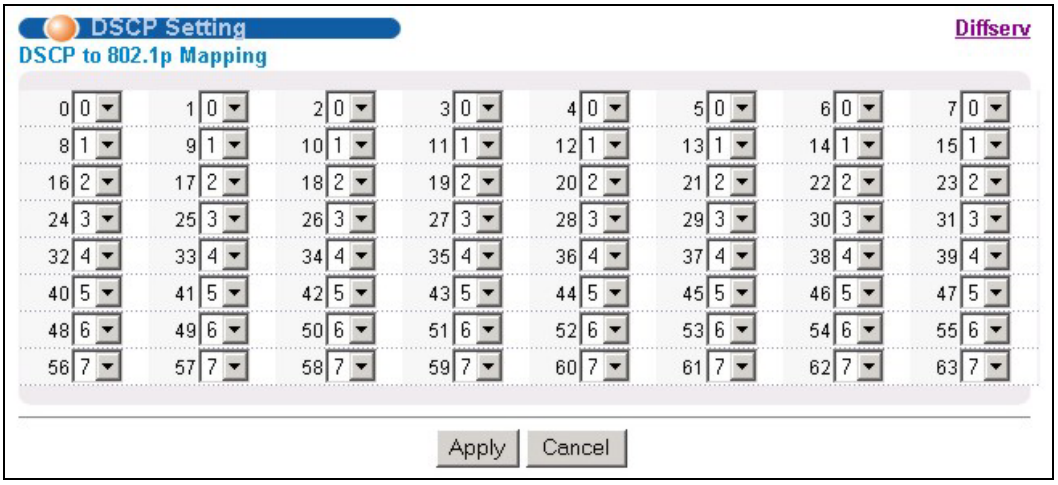


Figure 19-6 DiffServ: DSCP Setting

The following table describes the labels in this screen.

Table 19-5 DiffServ: DSCP Setting

LABEL	DESCRIPTION
0 … 63	This is the DSCP classification identification number. To set the IEEE802.1p priority mapping, select the priority level from the drop-down list box.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard all changes and start configuring the screen again.

Chapter 20 Queuing Method

This chapter introduces SPQ and WFQ.

20.1 Introduction to Queuing

Queuing is used to help solve performance degradation when there is network congestion. Use the **Queuing Method** screen to configure queuing algorithms for outgoing traffic. See also **Priority Queue Assignment** in **Switch Setup** and **802.1p Priority** in **Port Setup** for related information.

Queuing algorithms allow switches to maintain separate queues for packets from each individual source or flow and prevent a source from monopolizing the bandwidth.

The switch has four physical queues, Q0 to Q3. Q3 has the highest priority and Q0 has the lowest.

Table 20-1 Physical Queue Priority

QUEUE	PRIORITY
Q3	1 (Highest)
Q2	2
Q1	3
Q0	4 (Lowest)

20.1.1 Strict Priority Queuing (SPQ)

Strict Priority Queuing (SPQ) services queues based on priority only. As traffic comes into the switch, traffic on the highest priority queue, Q3 is transmitted first. When that queue empties, traffic on the next highest-priority queue, Q2 is transmitted until Q2 empties, and then traffic is transmitted on Q1 and so on. If higher priority queues never empty, then traffic on lower priority queues never gets sent. SPQ does not automatically adapt to changing network requirements.

20.1.2 Weighted Fair Queuing (WFQ)

Weighted Fair Queuing (WFQ) services queues based on their priority and queue weight (the number you configure in the **%** field – see *Figure 20-1*). WFQ is activated only when a port has more traffic than it can handle. Queues with larger weights get more service than queues with smaller weights. This queuing mechanism is highly efficient in that it divides any available bandwidth across the different traffic queues.

20.2 Configuring Queuing

Click **Advanced Application**, **Queuing Method** in the navigation panel.

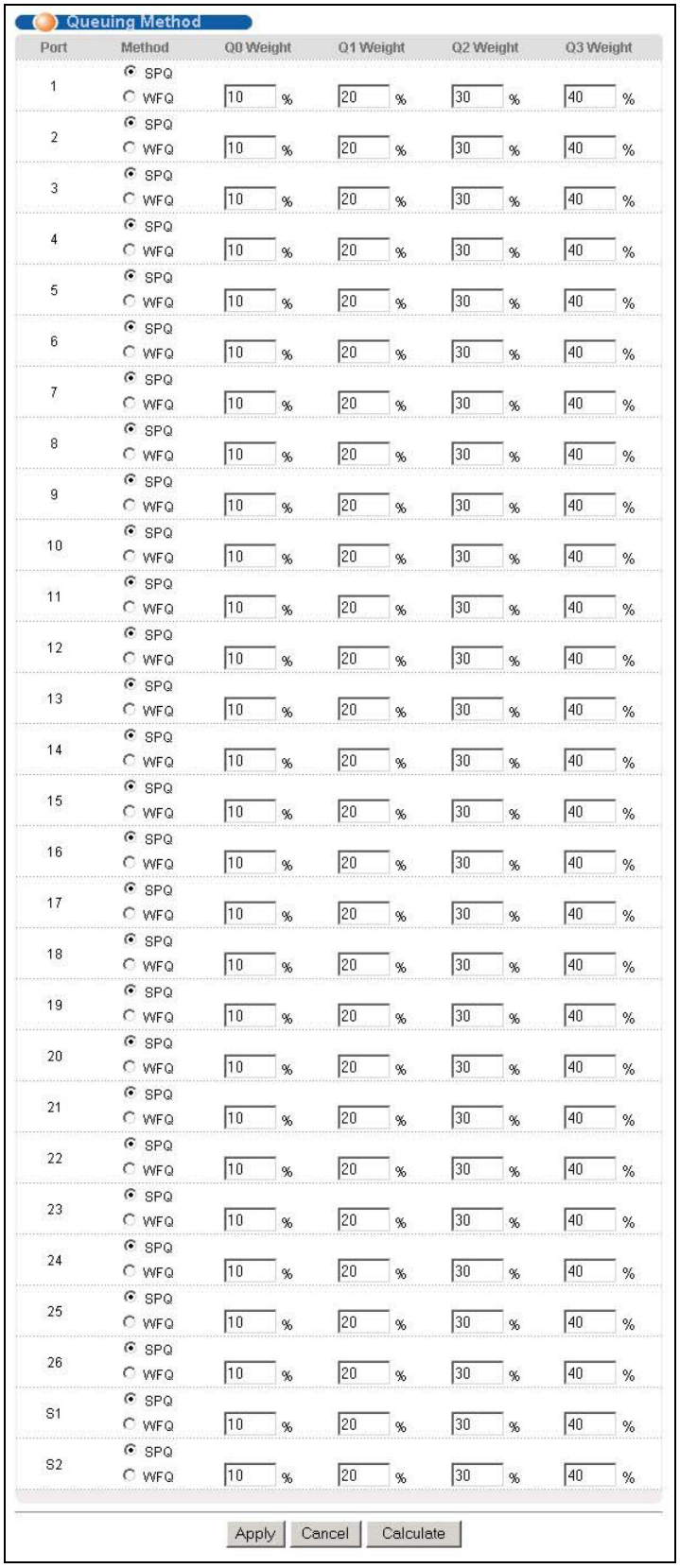


Figure 20-1 Queuing Method

The following table describes the labels in this screen.

Table 20-2 Queuing Method

LABEL	DESCRIPTION
Port	This label shows the port you are configuring.
Method	Select **SPQ** (Strict Priority Queuing) or **WFQ** (Weighted Fair Queuing). Strict Priority Queuing (SPQ) services queues based on priority only. When the highest priority queue empties, traffic on the next highest-priority queue begins. Q3 has the highest priority and Q0 the lowest. Weighted Fair Queuing (WFQ) services queues based on their priority and queue weight (the number you configure in the queue **%** field). Queues with larger weights get more service than queues with smaller weights.
Q0~Q3 Weight %	When you select **WFQ,** enter the queue weight here. Bandwidth is divided across the different traffic queues according to their weights. Queues with larger weights get more service than queues with smaller weights.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Calculate	Click **Calculate** to make sure the WFQ queuing weights total to 100%; if not an error message is displayed.

Chapter 21 VRRP

This chapter shows you how to configure and monitor the Virtual Routing Redundancy Protocol (VRRP) on the ES.

21.1VRRP Overview

Each host on a network is configured to send packets to a statically configured default gateway (the ES). The default gateway can become a single point of failure. Virtual Routing Redundancy Protocol (VRRP), defined in RFC 2338, allows you to create redundant backup gateways to ensure that the default gateway of a host is always available.

In VRRP, a virtual router (VR) represents a number of physical layer-3 devices. An IP address is associated with the virtual router. A layer-3 device having the same IP address is the preferred master router while the other Layer-3 devices are the backup routers. The master router forwards traffic for the virtual router. When the master router becomes unavailable, a backup router assumes the role of the master router until the master router comes back up and takes over.

The following figure shows a VRRP network example with the ES A and B implementing one virtual router VR1 to ensure the link between the host X and the uplink gateway G. Host X is configured to use VR1 (192.168.1.20) as the default gateway. If the ES A has a higher priority, it is the master router. ES B, having a lower priority, is the backup router.

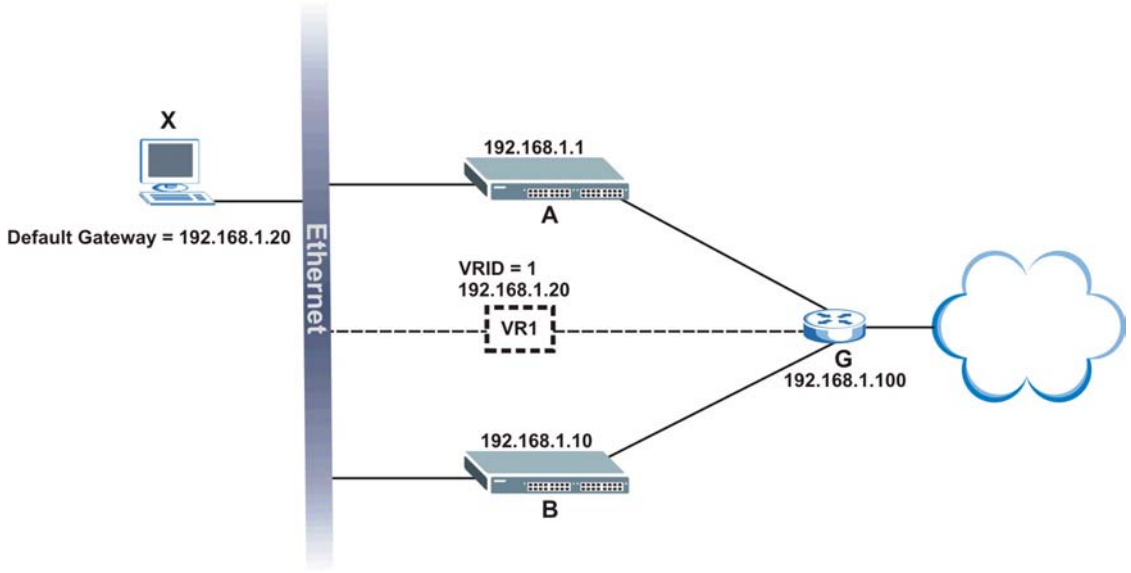


Figure 21-1 VRRP: Example 1

If the ES A (the master router) is unavailable, the ES B takes over. Traffic is then processed by switch B.

21.2Viewing VRRP Status

Click **Advanced Application**, **VRRP** in the navigation panel to display the **VRRP Status** screen as shown next.

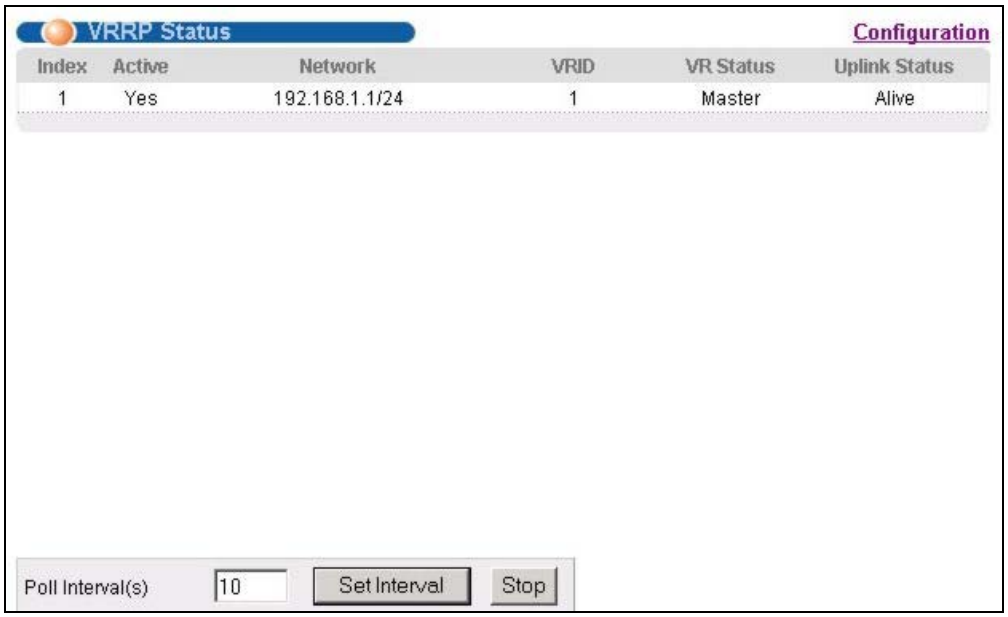


Figure 21-2 VRRP Status

The following table describes the labels in this screen.

Table 21-1 VRRP Status

LABEL	DESCRIPTION
Index	This field displays the index number of a rule.
Active	This field displays whether a rule is enabled (**Yes**) or disabled (**No**).
Network	This field displays the IP address and the subnet mask bits of an IP routing domain that is associated to a virtual router.
VRID	This field displays the ID number of the virtual router.
VR Status	This field displays the status of the virtual router. This field is **Master** indicating that the ES functions as the master router. This field is **Backup** indicating that the ES functions as a backup router. This field displays **Init** when the ES is initiating the VRRP protocol or when the **Uplink Status** field displays **Dead**.
Uplink Status	This field displays the status of the link between the ES and the uplink gateway. This field is **Alive** indicating that the link between the ES and the uplink gateway is up. Otherwise, this field is **Dead**. This field displays **Probe** when the ES is check for the link state.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.

Table 21-1 VRRP Status

LABEL	DESCRIPTION
Stop	Click **Stop** to halt system statistic polling.

21.3 Configuring VRRP

Follow the instructions in the follow sections to configure VRRP on the ES.

21.3.1 IP Interface Setup

Before configuring VRRP, first create an IP interface (or routing domain) in the **IP Setup** screen (see the section on IP setup for more information).)

Click **Advanced Application**, **VRRP** and click the **Configuration** link to display the **VRRP Configuration** screen as shown next.

You can only configure VRRP on interfaces with unique VLAN IDs.

Routing domains with the same VLAN ID are not displayed in the table indicated.

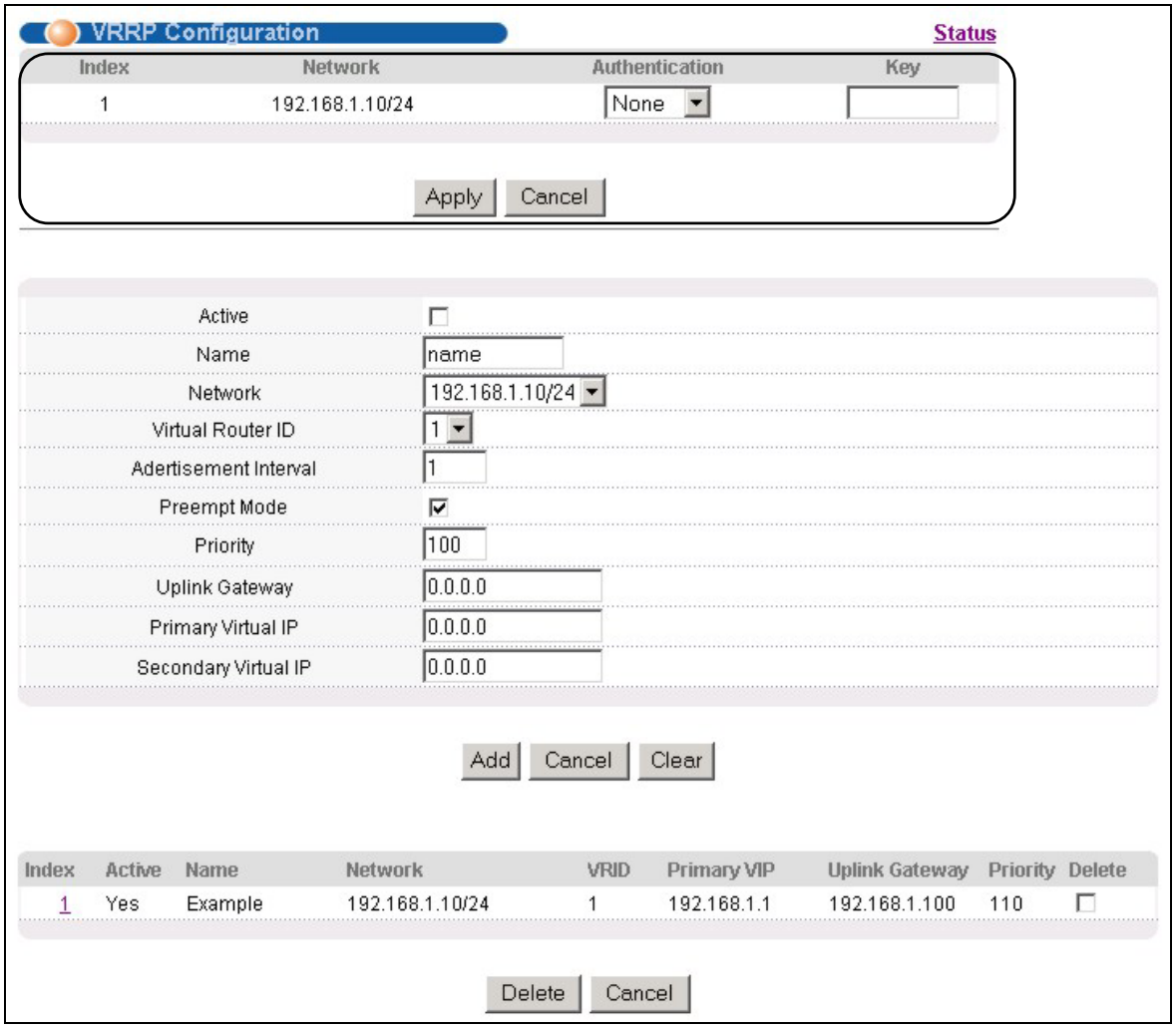


Figure 21-3 VRRP Configuration: IP Interface

The following table describes the labels in this screen.

Table 21-2 VRRP Configuration: IP Interface

LABEL	DESCRIPTION
Index	This field displays the index number of an entry.
Network	This field displays the IP address and number of subnet mask bit of an IP domain.
Authentication	Select **None** to disable authentication. This is the default setting. Select **Simple** to use a simple password to authenticate VRRP packet exchanges on this interface.
Key	When you select **Simple** in the **Authentication** field, enter a password key (up to eight printable ASCII character long) in this field.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard all changes made in this table.

21.3.2 VRRP Parameters

This section describes the VRRP parameters.

Advertisement Interval

The master router sends out Hello messages to let the other backup routers know that it is still up and running. The time interval between sending the Hello messages is the advertisement interval. By default, a Hello message is sent out every second.

If the backup routers do not receive a Hello message from the master router after this interval expires, it is assumed that the master router is down. Then the backup router with the highest priority becomes the master router.

All routers participating in the virtual router must use the same advertisement interval.

Priority

Configure the priority level (1 to 254) to set which backup router to take over in case the master router goes down. The backup router with the highest priority will take over. The priority of the VRRP router that owns the IP address(es) associated with the virtual router is 255.

Preempt Mode

If the master router is unavailable, a backup router assumes the role of the master router. However, when another backup router with a higher priority joins the network, it will preempt the lower priority backup router that is the master. Disable preempt mode to prevent this from happening.

By default, a layer 3 device with the same IP address as the virtual router will become the master router regardless of the preempt mode.

21.3.3 Configuring VRRP Parameters

After you set up an IP interface, configure the VRRP parameters.

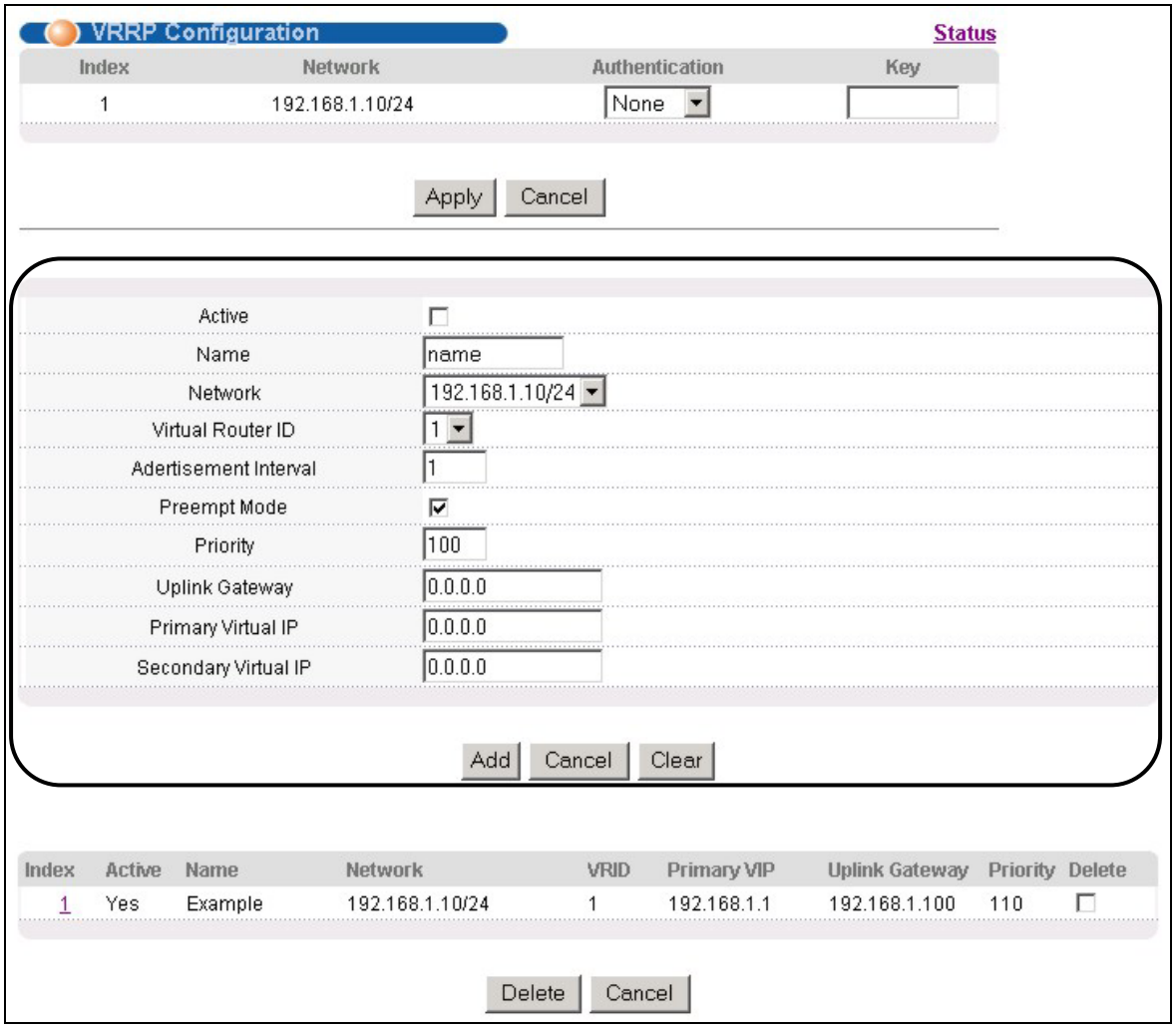


Figure 21-4 VRRP Configuring: VRRP Parameters

The following table describes the labels in this screen.

Table 21-3 VRRP Configuring: VRRP Parameters

LABEL	DESCRIPTION
Active	Select this option to enable this VRRP entry.
Name	Enter a descriptive name for this VRRP entry.
Network	Select an IP domain to which this VRRP entry applies.
Virtual Router ID	Select a virtual router number (1 to 7) for which this VRRP entry is created. You can configure up to seven virtual routers for one network.
Advertisement Interval	Specify the number of seconds between Hello message transmissions. The default is **1**.
Preempt Mode	Select this option to activate preempt mode.

Table 21-3 VRRP Configuring: VRRP Parameters

LABEL	DESCRIPTION
Priority	Enter a number (between 1 and 254) to set the priority level. The bigger the number, the higher the priority. This field is **100** by default.
Uplink Gateway	Enter the IP address of the uplink gateway in dotted decimal notation. The ES checks the link to the uplink gateway.
Primary Virtual IP	Enter the IP address of the primary virtual router in dotted decimal notation.
Secondary Virtual IP	This field is optional. Enter the IP address of a secondary virtual router in dotted decimal notation. This field is ignored when you enter **0.0.0.0**.
Add	Click **Add** to apply the changes.
Cancel	Click **Cancel** to discard all changes made in this table.
Clear	Click **Clear** to set the above fields back to the factory defaults.

21.4 VRRP Configuration Summary

To view a summary of all VRRP configurations on the ES, scroll down to the bottom of the **VRRP Configuration** screen.

Figure 21-5 VRRP Configuration: Summary

The following table describes the labels in this screen.

Table 21-4 VRRP Configuring: VRRP Parameters

LABEL	DESCRIPTION
Index	This field displays the index number of an entry.
Active	This field shows whether a VRRP entry is enabled (**Yes**) or disabled (**No**).
Name	This field displays a descriptive name of an entry.
Network	This field displays the IP address and subnet mask of an interface.
VRID	This field displays the ID number of a virtual router.
Primary VIP	This field displays the IP address of the primary virtual router.
Uplink Gateway	This field displays the IP address of the uplink gateway.
Priority	This field displays the priority level (1 to 255) of the entry.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

21.5VRRP Configuration Examples

The following sections show two VRRP configuration examples on the ES.

21.5.1 One Subnet Network Example

The figure below shows a simple VRRP network with only one virtual router VR1 (VRID =1) and two switches. The network is connected to the WAN via an uplink gateway G (192.168.1.100). The host computer X is set to use VR1 as the default gateway.

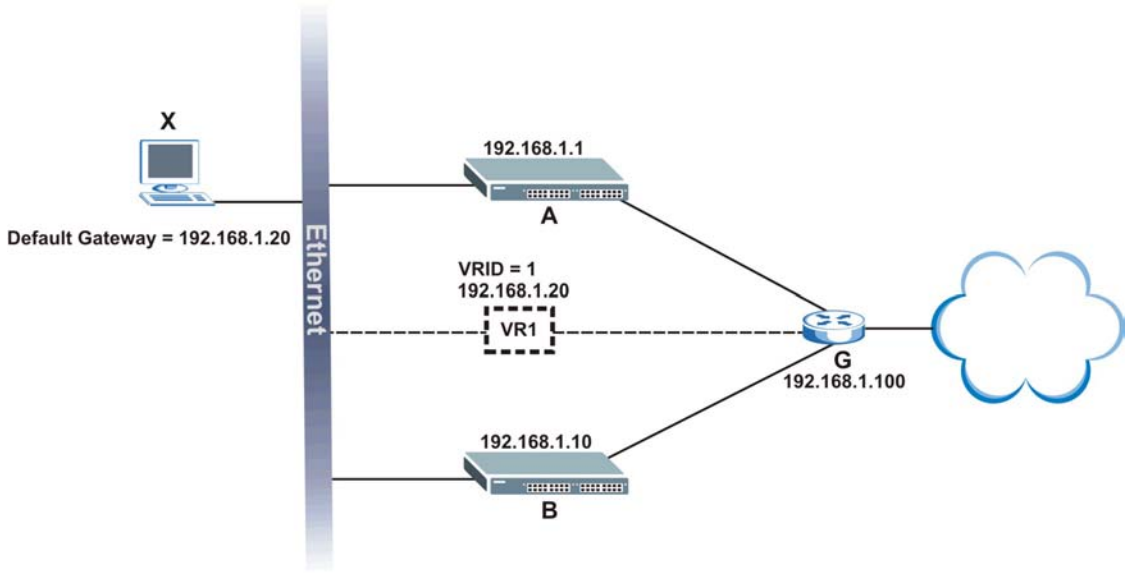


Figure 21-6 VRRP Configuration Example: One Virtual Router Network

You want to set switch A as the master router. Configure the VRRP parameters in the **VRRP Configuration** screens on the ESes as shown in the figures below.

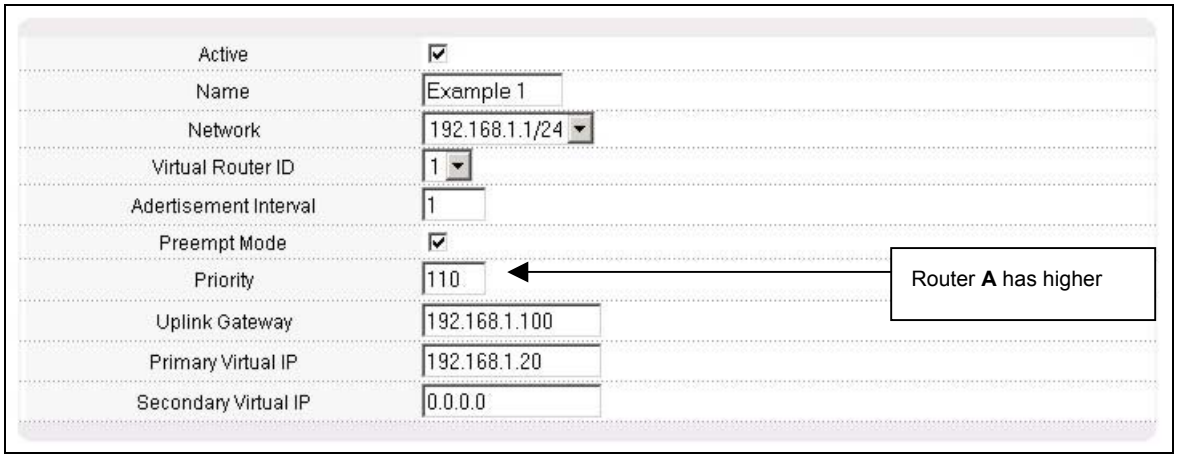


Figure 21-7 VRRP Example 1: VRRP Parameter Settings on Switch A

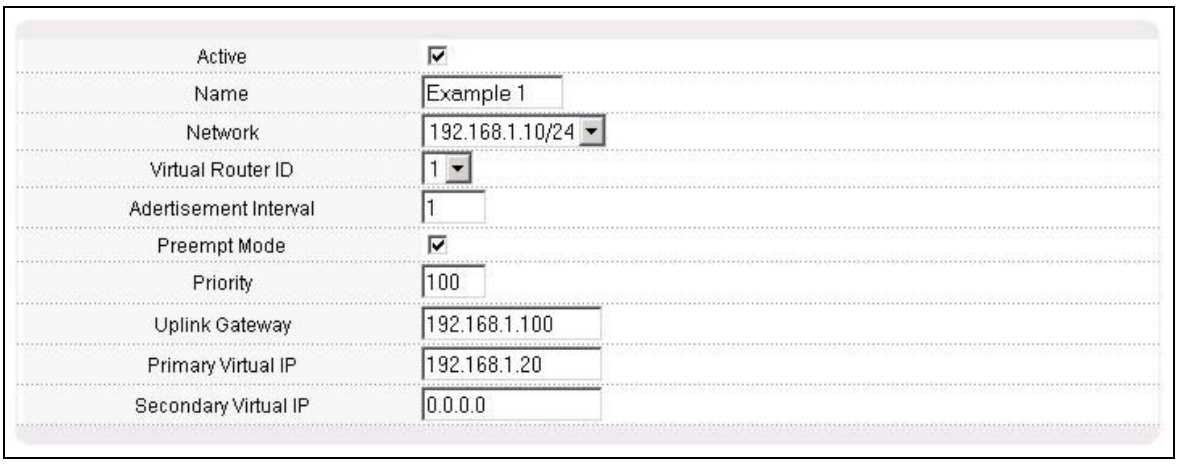


Figure 21-8 VRRP Example 1: VRRP Parameter Settings on Switch B

After configuring and saving the VRRP configuration, the **VRRP Status** screens for both switches are shown next.

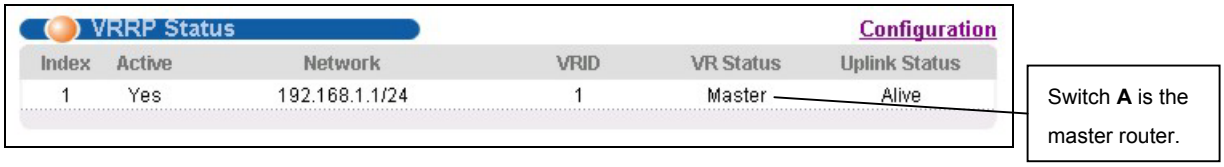


Figure 21-9 VRRP Example 1: VRRP Status on Switch A

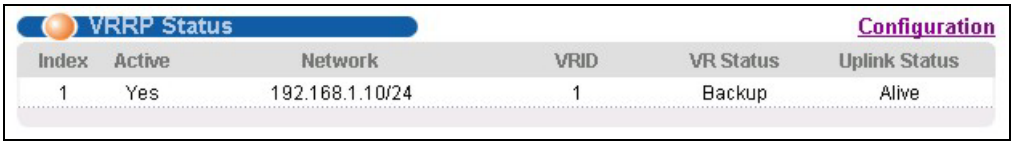


Figure 21-10 VRRP Example 1: VRRP Status on Switch B

21.5.2 Two Subnets Example

The following figure depicts an example in which two switches share the network traffic. Hosts in the two network groups use different default gateways. Each switch is configured to backup a virtual router using VRRP.

You wish to configure switch A as the master router for virtual router VR1 and as a backup for virtual router VR2. On the other hand, switch B is the master for VR2 and a backup for VR1.

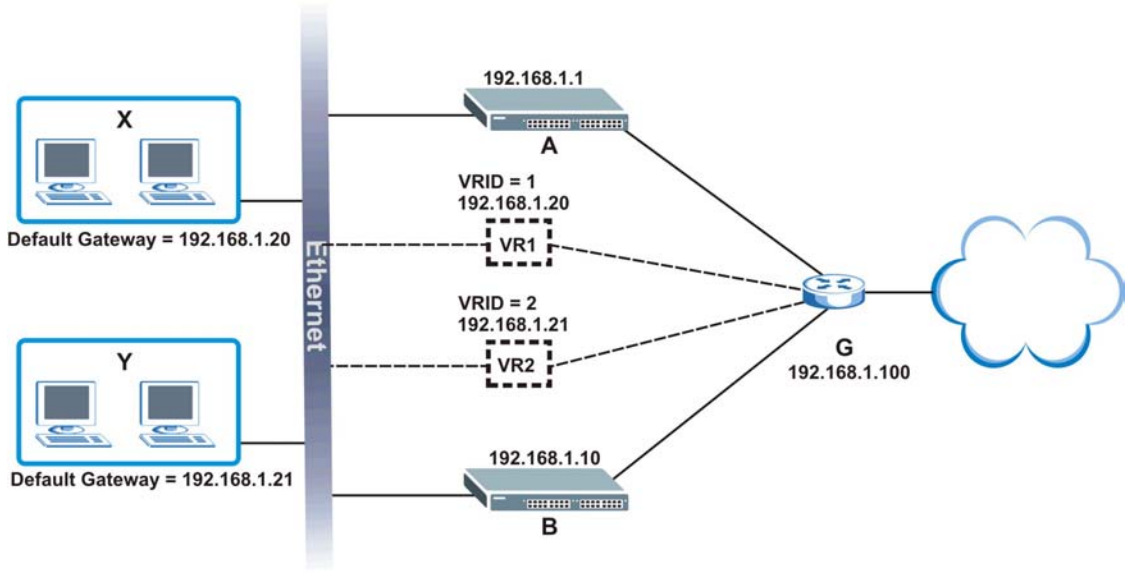


Figure 21-11 VRRP Configuration Example: Two Virtual Router Network

Keeping the VRRP configuration in example 1 for virtual router VR1 (refer to *Section 21.5.1*), you need to configure the **VRRP Configuration** screen for virtual router VR2 on each switch. Configure the VRRP parameters on the ESes as shown in the figures below.

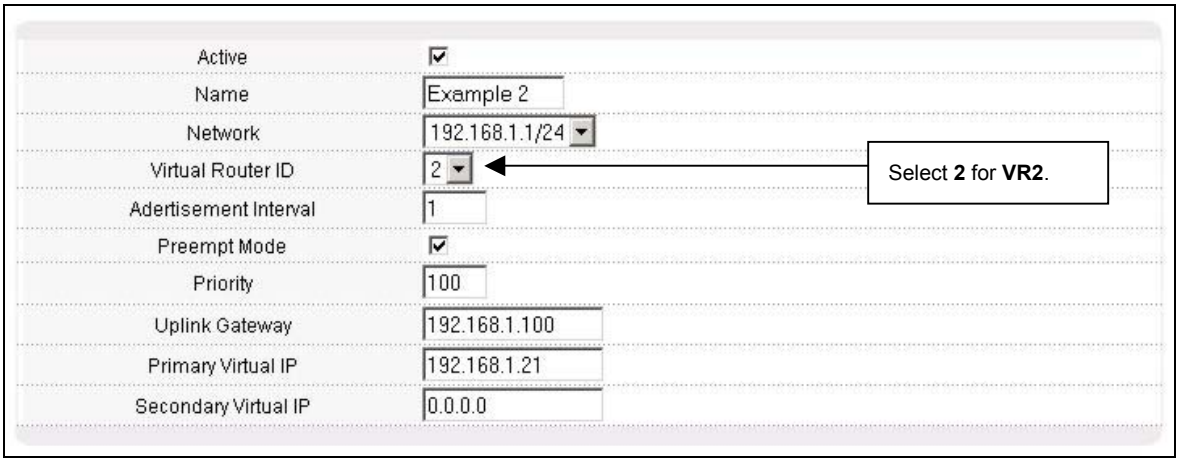


Figure 21-12 VRRP Example 2: VRRP Parameter Settings for VR2 on Switch A

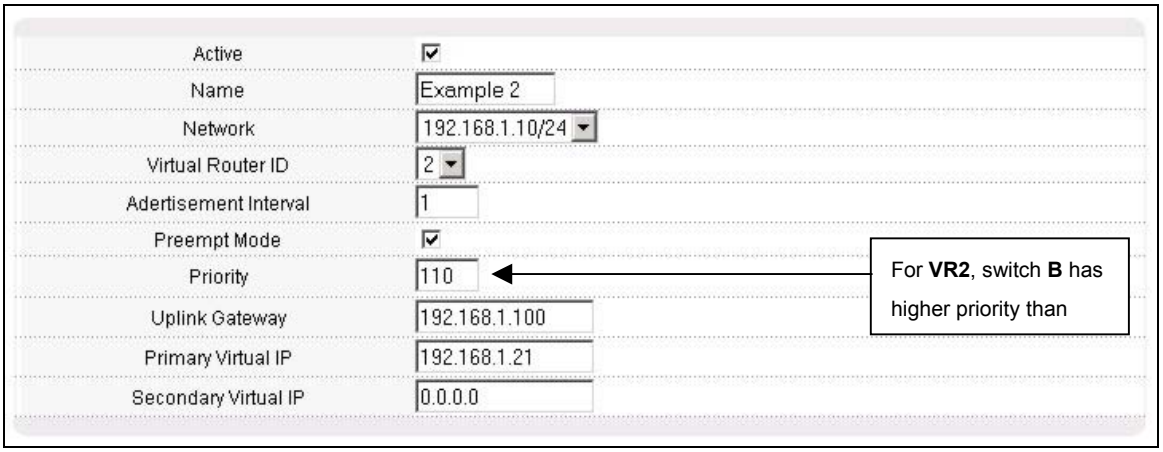


Figure 21-13 VRRP Example 2: VRRP Parameter Settings for VR2 on Switch B

After configuring and saving the VRRP configuration, the **VRRP Status** screens for both switches are shown next.

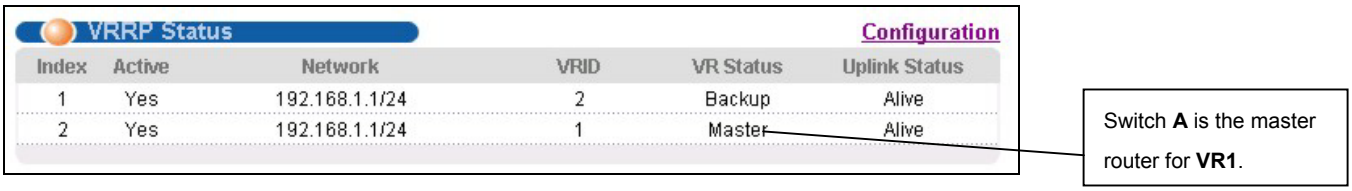


Figure 21-14 VRRP Example 2: VRRP Status on Switch A

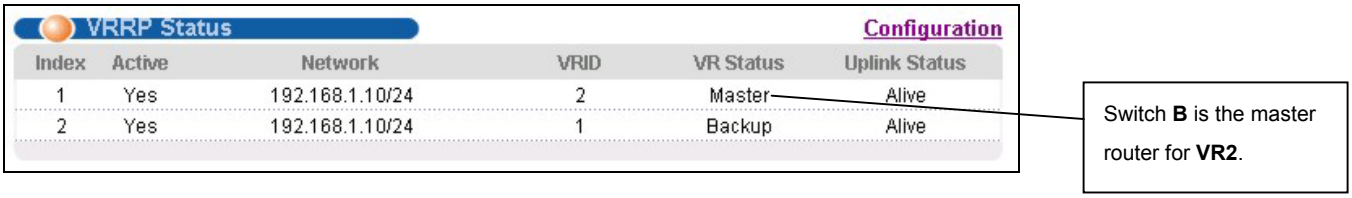


Figure 21-15 VRRP Example 2: VRRP Status on Switch B

Part V

Routing Protocol

This part describes the Routing Protocol screens.

Chapter 22 Static Route

This chapter shows you how to configure static routes.

22.1 Configuring Static Routes

Static routes tell the ES-4024 how to forward IP traffic when you configure the TCP/IP parameters manually.

Click **Routing Protocol**, **Static Routing** in the navigation panel to display the screen as shown.

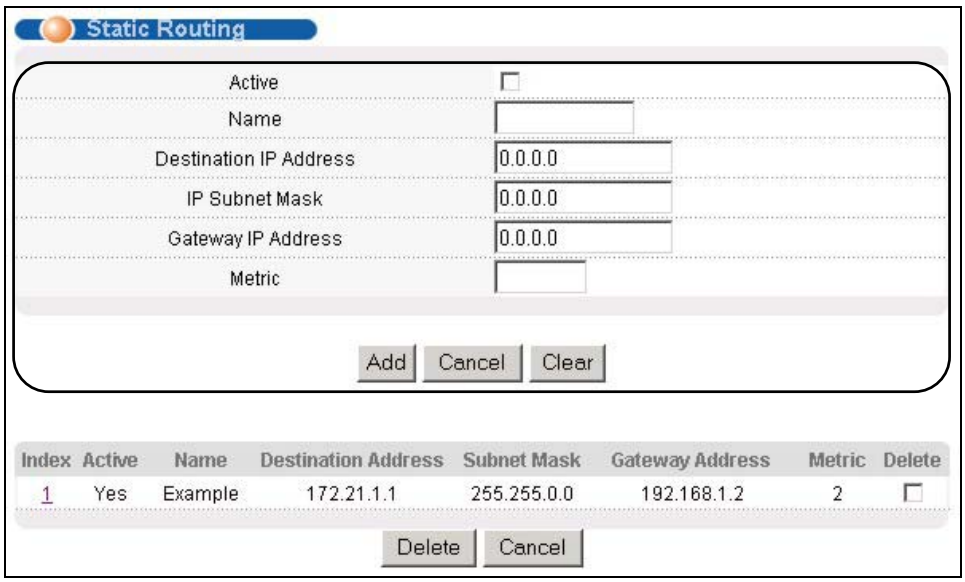


Figure 22-1 Static Routing

The following table describes the related labels you use to create a static route.

Table 22-1 Static Routing

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route.
Name	Enter a descriptive name for this route. This is for identification purpose only.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the subnet mask for this destination.

Table 22-1 Static Routing

LABEL	DESCRIPTION
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your switch that will forward the packet to the destination. The gateway must be a router on the same segment as your switch.
Metric	The metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Add	Click **Add** to insert a new static route.
Cancel	Click **Cancel** to reset the above fields to your previous configuration.
Clear	Click **Clear** to set the above fields back to the factory defaults.

22.1.1 View Static Route Configurations

View the current static routes on the switch in the summary table at the bottom of the **Static Routing** screen.

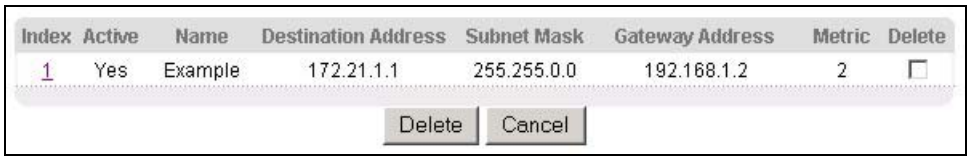


Figure 22-2 Static Routing: Summary Table

The following table describes the labels in the summary table.

Table 22-2 Static Routing: Summary Table

LABEL	DESCRIPTION
Index	This field displays the index number of the route. Click a number to edit the static route entry.
Active	This field displays **Yes** when the static route is activated and **NO** when it is deactivated.
Name	This field displays the descriptive name for this route. This is for identification purpose only.
Destination Address	This field displays the IP network address of the final destination.
Subnet Mask	This field displays the subnet mask for this destination.
Gateway Address	This field displays the IP address of the gateway. The gateway is an immediate neighbor of your switch that will forward the packet to the destination.
Metric	This field displays the cost of transmission for routing purposes.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

Chapter 23 RIP

This chapter shows you how to configure RIP (Routing Information Protocol).

23.1 Overview

RIP (Routing Information Protocol) allows a routing device to exchange routing information with other routers. The **Direction** field controls the sending and receiving of RIP packets. When set to:

1. **Both -** the ES-4024 will broadcast its routing table periodically and incorporate the RIP information that it receives.
2. **Incoming -** the ES-4024 will not send any RIP packets but will accept all RIP packets received.
3. **Outgoing -** the ES-4024 will send out RIP packets but will not accept any RIP packets received.
4. **None -** the ES-4024 will not send any RIP packets and will ignore any RIP packets received.

The **Version** field controls the format and the broadcasting method of the RIP packets that ES-4024 sends (it recognizes both formats when receiving). **RIP-1** is universally supported; but RIP-2 carries more information. **RIP-1** is probably adequate for most networks, unless you have an unusual network topology.

Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting.

23.2 Configuring RIP

Click **Routing Protocol**, **RIP** in the navigation panel to display the screen as shown. You cannot manually configure a new entry. Each entry in the table is automatically created when you configure a new IP domain in the **IP Setup** screen (refer to the section on IP routing domain setup).

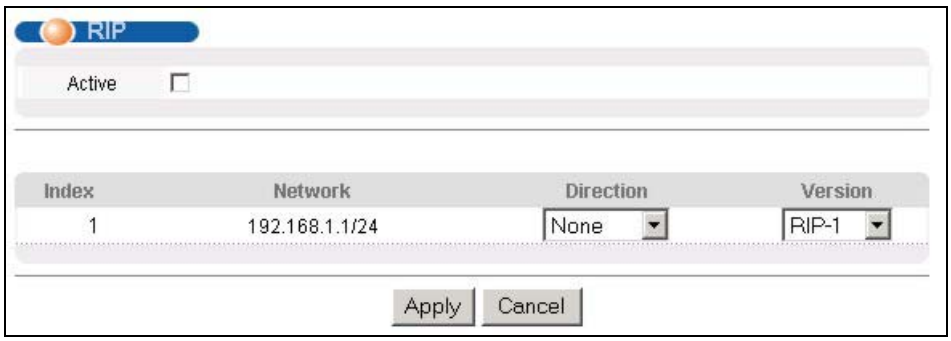


Figure 23-1 RIP

The following table describes the labels in this screen.

Table 23-1 RIP

LABEL	DESCRIPTION
Active	Select this check box to enable RIP on the switch.
Index	This field displays the index number of the entry.
Network	This field displays the IP domain configured on the switch. Refer to the section on IP Setup for more information on configuring IP domains.
Direction	Select the RIP direction from the drop-down list box. Choices are **Outgoing**, **Incoming**, **Both** and **None**.
Version	Select the RIP version from the drop-down list box. Choices are **RIP-1**, **RIP-2B** and **RIP-2M**.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring the fields again.

Chapter 24 IGMP

This chapter shows you how to configure IGMP.

24.1 Overview

IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a multicast group - it is not used to carry user data. Refer to *RFC 1112* and *RFC 2236* for information on IGMP versions 1 and 2 respectively.

The ES-4024 supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). At start up, the ES-4024 queries all directly connected networks to gather group membership. After that, the ES-4024 periodically updates this information.

24.2 Configuring IGMP

Click **Routing Protocol**, **IGMP** in the navigation panel to display the screen as shown next. Each entry in the table is automatically created when you configure a new IP domain in the **IP Setup** screen (refer to the section on IP routing domain setup).

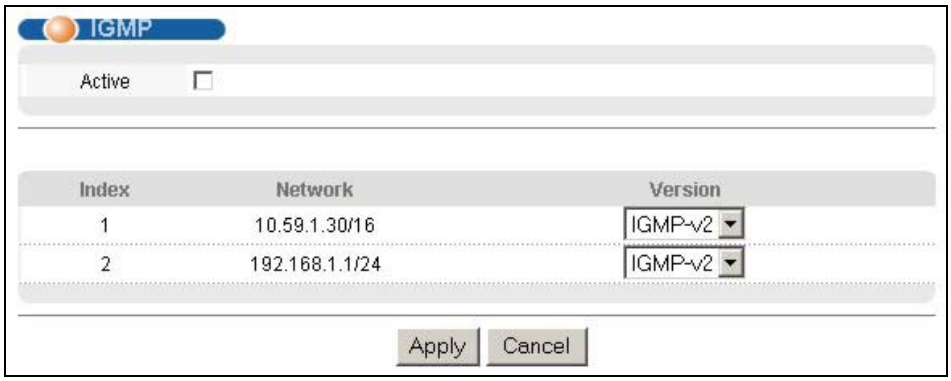


Figure 24-1 IGMP

The following table describes the labels in this screen.

Table 24-1 IGMP

LABEL	DESCRIPTION
Active	Select this check box to enable IGMP on the switch. **You *cannot* enable both IGMP snooping and IGMP at the same time. Refer to the section on IGMP snooping.**
Index	This field displays an index number of an entry.

Table 24-1 IGMP

LABEL	DESCRIPTION
Network	This field displays the IP domain configured on the switch. Refer to the *IP Setup* section for more information on configuring IP domains.
Version	Select an IGMP version from the drop-down list box. Choices are **IGMP-v1**, **IGMP-v2** and **None**.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring the fields again.

Chapter 25 DVMRP

This chapter introduces DVMRP and tells you how to configure it.

25.1 Introduction to DVMRP

DVMRP (Distance Vector Multicast Routing Protocol) is a protocol used for routing multicast data within an autonomous system (AS). This DVMRP implementation is based on draft-ietf-idmr-dvmrp-v3-10. DVMRP provides multicast forwarding capability to a layer 3 switch that runs both the IPv4 protocol (with IP Multicast support) and the IGMP protocol. The DVMRP metric is a hop count of 32.

IGMP is a protocol used for joining or leaving a multicast group. You must have IGMP enabled when you enable DVMRP; otherwise you see the screen as in *Figure 25-3*.

25.2 How DVMRP Works

DVMRP uses the Reverse Path Multicasting (RPM) algorithm to generate an IP Multicast delivery tree. Multicast packets are forwarded along these multicast tree branches. DVMRP dynamically learns host membership information using Internet Group Multicast Protocol (IGMP). The trees are updated dynamically to track the membership of individual groups.

Initially an advertisement multicast packet is broadcast (“B” in the following figure).

DVMRP-enabled Layer 3 devices that do not have any hosts in their networks that belong to this multicast group send back a prune message (“P”).

If hosts later join the multicast group, a graft message (“G”) to undo the prune is sent to the parent.

The final multicast (“M”) after pruning and grafting is shown in the next figure.

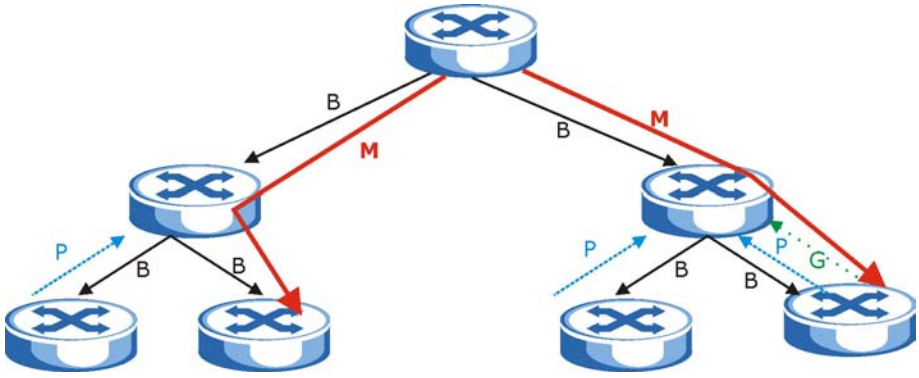


Figure 25-1 How DVMRP Works

25.2.1 DVMRP Terminology

DVMRP probes are used to discover other DVMRP Neighbors on a network.

DVMRP reports are used to exchange DVMRP source routing information. These packets are used to build the DVMRP multicast routing table that is used to build source trees and also perform Reverse Path Forwarding (RPF) checks on incoming multicast packets. RPF checks prevent duplicate packets being filtered when loops exist in the network topology.

DVMRP prunes trim the multicast delivery tree(s). DVMRP grafts attach a branch back onto the multicast delivery tree.

25.3 Configuring DVMRP

Configure DVMRP on the switch when you wish it to act as a multicast router ("mrouter"). Click **Routing Protocol**, **DVMRP** in the navigation panel to display the screen as shown.

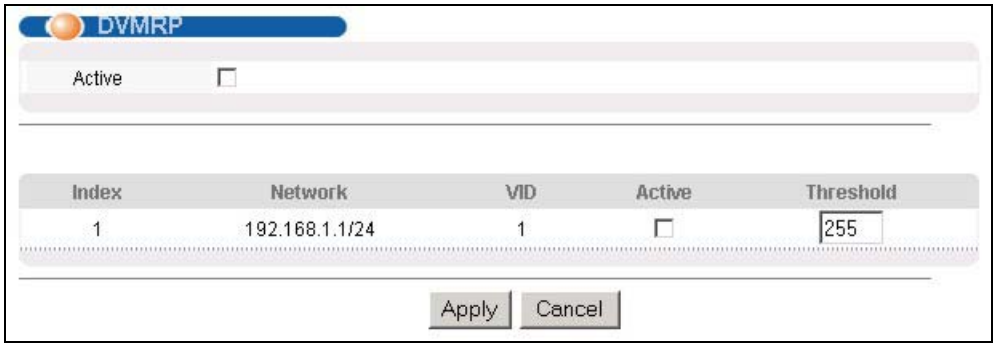


Figure 25-2 DVMRP

The following table describes the labels in this screen.

Table 25-1 DVMRP

LABEL	DESCRIPTION
Active	Select **Active** to enable DVMRP on the switch. You should do this if you want the switch to act as a multicast router.
Index	Index is the DVMRP configuration for the IP routing domain defined under **Network**. The maximum number of DVMRP configurations allowed is the maximum number of IP routing domains allowed on the switch. See the **IP Setup** chapter for more information on IP routing domains.
Network	This is the IP routing domain IP address and subnet mask you set up in **IP Setup.**
VID	DVMRP cannot be enabled on the same VLAN group across different IP routing domains, that is, you cannot have duplicate VIDs for different DVMRP configurations (see *Figure 25-5*).
Active	Select **Active** to enable DVMRP on this IP routing domain.
Threshold	Threshold is the maximum time to live (TTL) value. TTL is used to limit the scope of multicasting. You should reduce this value if you do not wish to flood Layer 3 devices many hops away with multicast traffic. This applies only to multicast traffic this switch sends out.
Apply	Click **Apply** to save these changes to the switch.

Table 25-1 DVMRP

LABEL	DESCRIPTION
Cancel	Click **Cancel** to begin configuring this part of the screen afresh.

25.3.1 DVMRP Configuration Error Messages

You must have IGMP enabled when you enable DVMRP; otherwise you see the screen as in the next figure.

Figure 25-3 IGMP Not Set Error

When you disable IGMP, but DVMRP is still active you also see another warning screen.

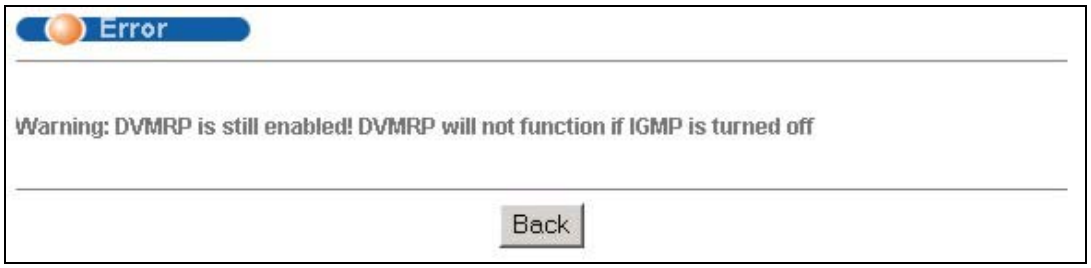


Figure 25-4 Unable to Disable IGMP Error

Each IP routing domain DVMRP configuration must be in a different VLAN group; otherwise you see the following screen.

Figure 25-5 No Duplicate VID Error Message

25.4 Default DVMRP Timer Values

The following are some default DVMRP timer values. These may be changed using line commands. Please see the commands chapter later in this User's Guide.

Table 25-2 Default DVMRP Timer Values

DVMRP FIELD	DEFAULT VALUE
Probe interval	10 sec
Report interval	35 sec
Route expiration time	140 sec
Prune lifetime	Variable (less than two hours)
Prune retransmission time	3 sec with exponential back off
Graft retransmission time	5 sec with exponential back off

Chapter 26 OSPF

This chapter describes the OSPF (Open Shortest Path First) routing protocol and shows you how to configure OSPF on the ES.

26.1 OSPF Overview

OSPF (Open Shortest Path First) is a link-state protocol designed to distribute routing information within an autonomous system (AS). An autonomous system is a collection of networks using a common routing protocol to exchange routing information.

OSPF offers some advantages over traditional vector-space routing protocols (such as RIP). The following table summarizes some of the major differences between OSPF and RIP.

Figure 26-1 OSPF vs. RIP

	OSPF	RIP
Network Size	Large	Small (with up to 15 routers)
Metrics	Bandwidth, hop count, throughput, round trip time and reliability.	Hop count
Convergence	Fast	Slow

26.1.1 OSPF Autonomous Systems and Areas

An OSPF autonomous system can be divided into logical areas. Each area represents a group of adjacent networks. All areas are connected to a backbone (also known as area 0). The backbone is the transit area to route packets between two areas. A stub area, at the edge of an AS, is not a transit area since there is only one connection to the stub area.

The following table describes the four classes of OSPF routers.

Table 26-1 OSPF Router Types

TYPE	DESCRIPTION
Internal Router (IR)	An Internal or intra-area router is a router in an area.
Area Border Router (ABR)	An Area Border Router connects two or more areas.
Backbone Router (BR)	A backbone router has an interface to the backbone.
AS Boundary Router	An AS boundary router exchanges routing information with routers in other ASes.

The following figure depicts an OSPF network example. The backbone is area 0 with a backbone router. The internal routers are in area 1 and 2. The area border routers connect area 1 and 2 to the backbone.

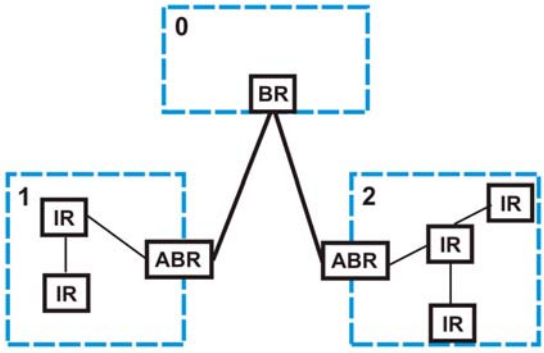


Figure 26-2 OSPF Network Example

26.1.2 How OSPF Works

Layer 3 devices exchange routing information to build synchronized link state database within the same AS or area. They do this by exchanging Hello messages to confirm which neighbor (layer 3) devices exist and then they exchange database descriptions (DDs) to create the link state database. The link state database in constantly updated through LSAs (Link State Advertisements).

The link state database contains records of router IDs, their associated links and path costs. Each device can then use the link state database and Dijkstra algorithm to compute the least cost paths to network destinations.

26.1.3 Interfaces and Virtual Links

An OSPF interface is a link between a layer 3 device and an OSPF network. An interface has state information, an IP address and subnet mask associated with it. When you configure an OSPF interface, you first set an interface to transmit OSPF traffic and add the interface to an area.

You can configure a virtual link to establish/maintain connectivity between a non-backbone area and the backbone. The virtual ink must be configured on both layer 3 devices in the non-backbone area and the backbone.

26.1.4 Configuring OSPF

To configure OSPF on the ES, do the following tasks

- Enable OSPF
- Create OSPF areas
- Create and associate interface(s) to an area
- Create virtual links to maintain backbone connectivity.

26.2 OSPF Status

To view current OSPF status, click **Routing Protocol**, **OSPF** in the navigation panel to display the screen as shown next.

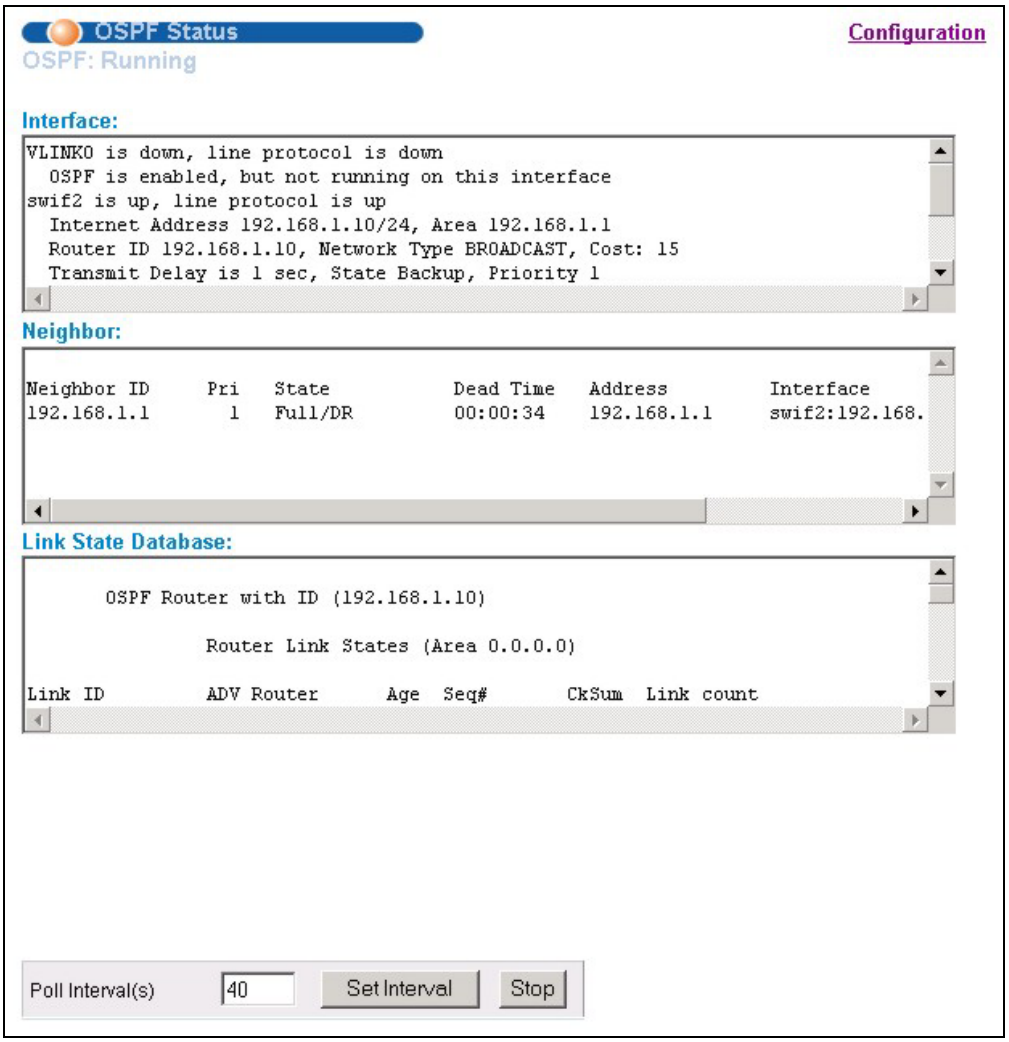


Figure 26-3 OSPF Status

The following table describes the labels in this screen.

Table 26-2 OSPF Status

LABEL	DESCRIPTION
OSPF	This field displays whether OSPF is activated (**Running**) or not (**Down**).
Interface	The text box displays the OSPF status of the interface(s) on the ES.
Neighbor	The text box displays the status of the neighboring router participating in the OSPF network.
Link State Database	The text box displays information in the link state database which contains data in the LSAs.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.

Table 26-2 OSPF Status

LABEL	DESCRIPTION
Stop	Click **Stop** to end OSPF status polling.

The following table describes some common output fields.

Table 26-3 OSPF Status: Common Output Fields

FIELD	DESCRIPTION
Interface	
Internet Address	This field displays the IP address and subnet bits of an IP routing domain.
Area	This field displays the area ID.
Router ID	This field displays the unique ID of the ES.
Transmit Delay	This field displays the transmission delay in seconds.
State	This field displays the state of the ES (**backup** or **DR** (designated router)).
Priority	This field displays the priority of the ES. This number is used in the designated router election.
Designated Router	This field displays the router ID of the designated router.
Backup Designated Router	This field displays the router ID of a backup designated router.
Time Intervals Configured	This field displays the time intervals (in seconds) configured.
Neighbor Count	This field displays the number of neighbor routers.
Adjacent Neighbor Count	This field displays the number of neighbor router(s) that is adjacent to the ES.
Neighbor	
Neighbor ID	This field displays the router ID of the neighbor.
Pri	This field displays the priority of the neighbor. This number is used in the designated router election.
State	This field displays the state of the neighbor (**backup** or **DR** (designated router)).
Dead Time	This field displays the dead time in seconds.
Address	This field displays the IP address of a neighbor.
Interface	This field displays the MAC address of a device.
Link State Database	
Link ID	This field displays the ID of a router or subnet.
ADV Router	This field displays the IP address of the layer-3 device that sends the LSAs.
Age	This field displays the time (in seconds) since the last LSA was sent.
Seq #	This field displays the link sequence number of the LSA.
Checksum	This field displays the checksum value of the LSA.
Link Count	This field displays the number of links in the LSA.

26.3 Enabling OSPF and General Settings

To activate OSPF and set general settings, click **Routing Protocols**, **OSPF** and the **Configuration** link to display the **OSPF Configuration** screen.

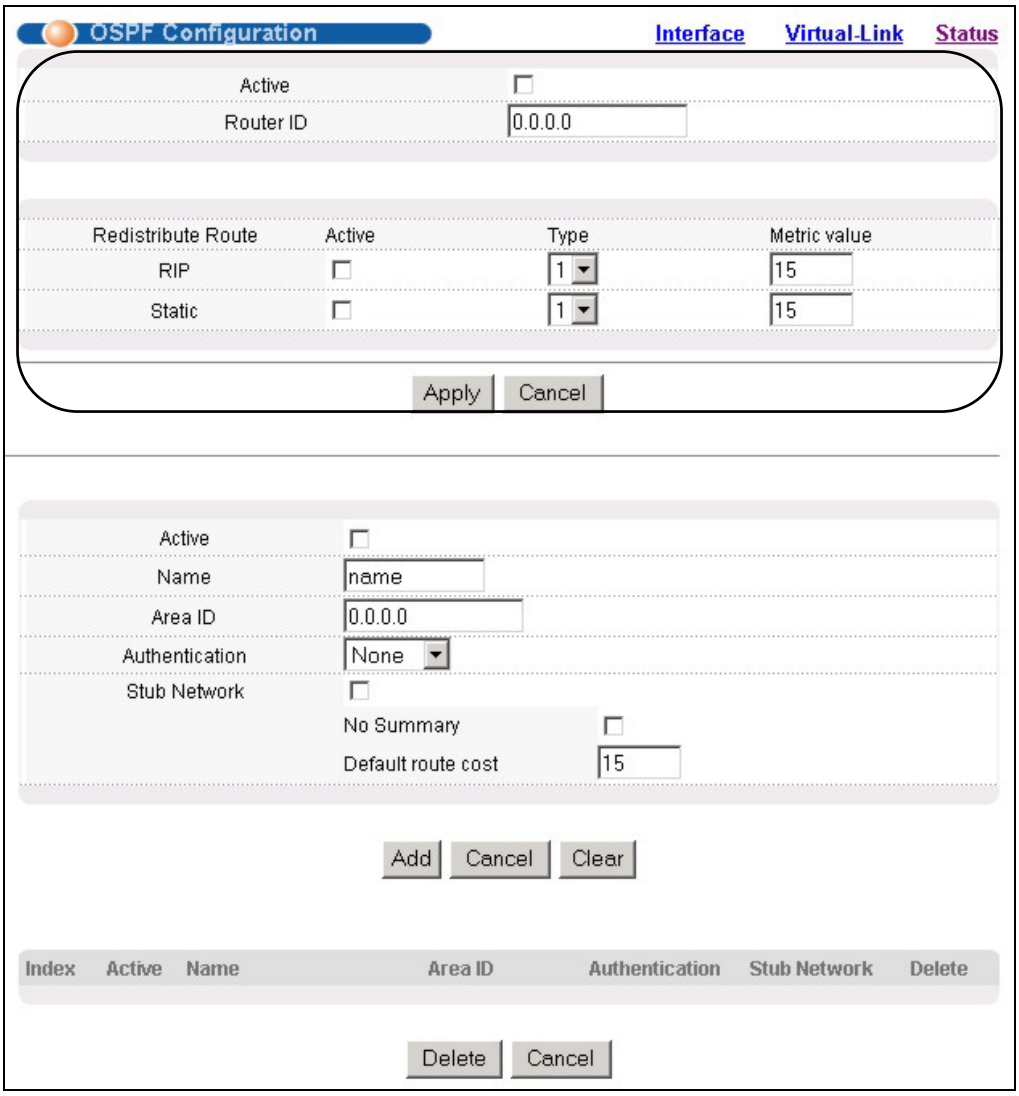


Figure 26-4 OSPF Configuration: Activating and General Settings

The follow table describes the related labels in this screen.

Table 26-4 OSPF Configuration: Activating and General Settings

LABEL	DESCRIPTION
Active	OSPF is disabled by default. Select this option to enable it.
Router ID	Router ID uniquely identifies the ES in an OSPF. Enter a unique ID (the IP address in dotted decimal notation) for the ES.
Redistribute Route	Route redistribution allows your ES to import and translate external routes learned through other routing protocols (**RIP** and **Static**) into the OSPF network transparently.
Active	Select this option to activate route redistribution for routes learn through the selected protocol.

Table 26-4 OSPF Configuration: Activating and General Settings

LABEL	DESCRIPTION
Type	Select **1** for routing protocols (such as RIP) whose external metrics are directly comparable to the internal OSPF cost. When selecting a path, the internal OSPF cost is added to the AB boundary router to the external metrics. Select **2** for routing protocols whose external metrics are not comparable to the OSPF cost. In this case, the external cost of the AB boundary router is used in path decision to a destination.
Metric Value	Enter a route cost (between 0 and 16777214).
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to start configuring the above fields again.

26.4 Configuring OSPF Areas

To ensure that the ES receives only routing information from a trusted layer 3 devices, activate authentication. The OSPF supports three authentication methods:

- None – no authentication is used.
- Simple – authenticate link state updates using an 8 printable ASCII character password.
- MD5 – authenticate link state updates using a 16 printable ASCII character password.

To configure a stub area, set the related fields in the **OSPF Configuration** screen.

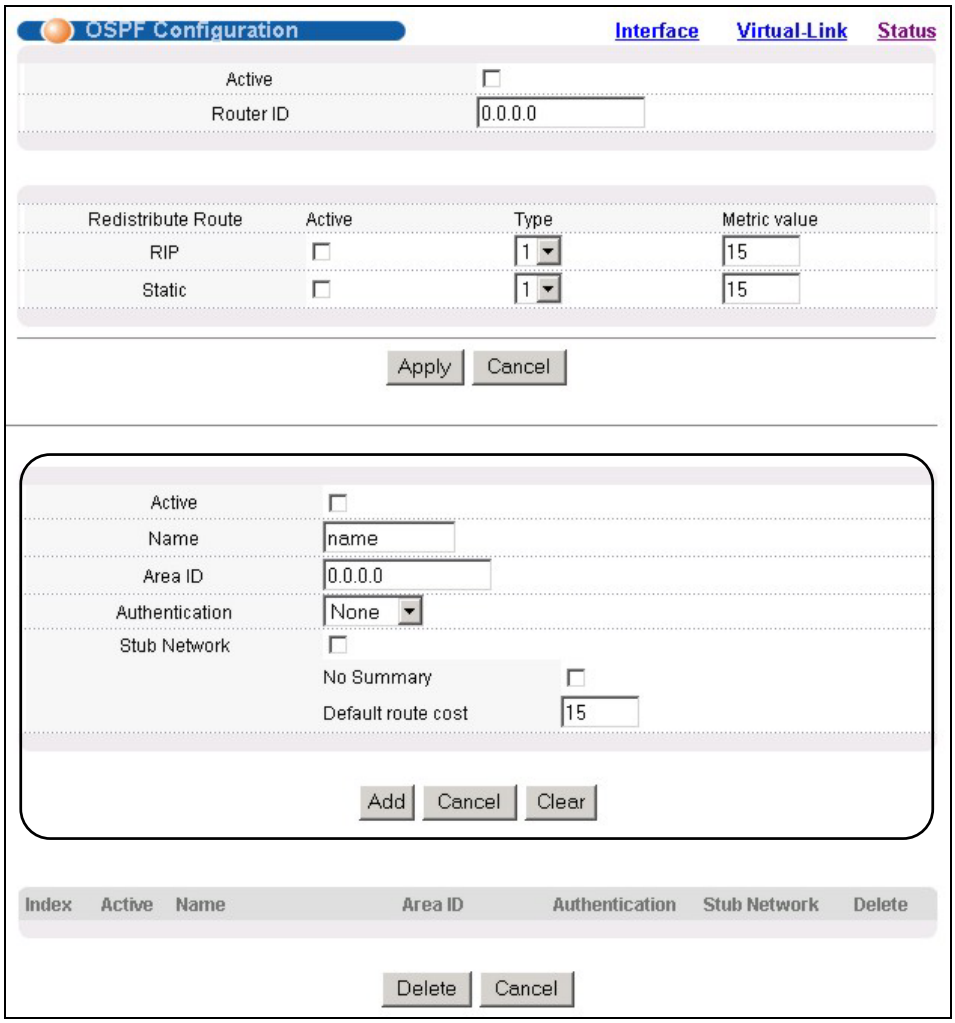


Figure 26-5 OSPF Configuration: Area Setup

The following table describes the related labels in this screen.

Table 26-5 OSPF Configuration: Area Setup

LABEL	DESCRIPTION
Active	Select this option to enable an area.
Name	Enter a descriptive name for an area.
Area ID	Enter an IP domain (in dotted decimal notation) that uniquely identifies a subnet. A value of **0.0.0.0** indicates that this is a backbone (also known as Area 0). You can create only one backbone area on the ES.
Authentication	Select an authentication method (**Simple** or **MD5**) to activate authentication. Select **None** to disable authentication. Interface(s) and virtual interface(s) must use the same authentication method as the associated area.
Stub Area	Select this option to set the area as a stub area. If you enter **0.0.0.0** in the **Area ID** field, the settings in the **Stub Area** fields are ignored.
No Summary	Select this option to set the ES to not send/receive LSAs.

Table 26-5 OSPF Configuration: Area Setup

LABEL	DESCRIPTION
Default Route Cost	Specify a cost (between 0 and 16777214) used to add a default route into a stub area for routes which are external to an OSPF domain. If you do not set a route cost, no default route is added.
Add	Click **Add** to apply the changes.
Cancel	Click **Cancel** to start configuring the above fields again.
Clear	Click **Clear** to set the above fields back to the factory defaults.

26.4.1 Viewing OSPF Area Information Table

The bottom of the **OSPF Configuration** screen displays a summary table of all the OSPF areas you have configured.

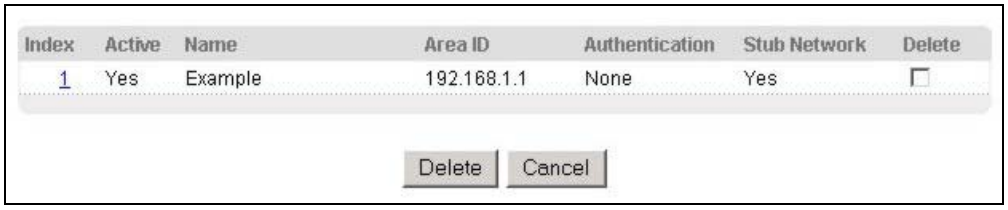


Figure 26-6 OSPF Configuration: Summary Table

The following table describes the related labels in this screen.

Table 26-6 OSPF Configuration: Summary Table

LABEL	DESCRIPTION
Index	This field displays the index number of an area.
Active	This field displays whether an area is enabled (**Yes**) or not (**No**).
Name	This field displays the descriptive name of an area.
Area ID	This field displays the IP domain that uniquely identifies an area. An area ID of **0.0.0.0** indicates the backbone.
Authentication	This field displays the authentication method used (**None**, **Simple** or **MD5**).
Stub Network	This field displays whether an area is a stub network (**Yes**) or not (**No**).
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

26.5 Configuring OSPF Interfaces

To configure an OSPF interface, first create an IP routing domain in the **IP Setup** screen (see the section on IP setup for more information). Once you create an IP routing domain, an OSPF interface entry is automatically created.

In the **OSPF Configuration** screen, click **Interface** to display the **OSPF Interface** screen.

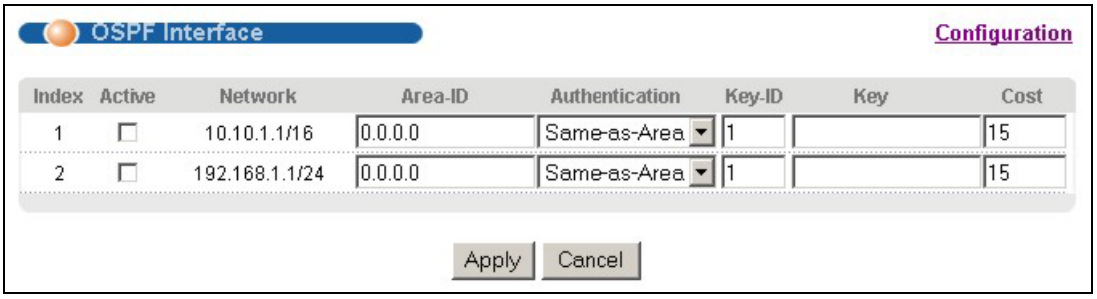


Figure 26-7 OSPF Interface

The following table describes the labels in this screen.

Table 26-7 OSPF Interface

LABEL	DESCRIPTION
Index	This field displays the index number for an interface.
Active	Select this option to enable an interface.
Network	This field displays the IP interface information.
Area-ID	Enter the IP domain (in dotted decimal notation) of an area to associate the interface to that area.
Authentication	**OSPF Interface(s) must use the same authentication method within the same area.** Select an authentication method. Choices are **Same-as-Area**, **None** (default), **Simple** and **MD5**. To participate in an OSPF network, you must set the authentication method and/or password the same as the associated area. Select **Same-as-Area** to use the same authentication method within the area and set the related fields when necessary. Select **None** to disable authentication. This is the default setting. Select **Simple** and set the **Key ID** and **Key** fields to authenticate OSPF packets transmitted through this interface using simple password authentication. Select **MD5** and set the **Key ID** and **Key** fields to authenticate OSPF packets transmitted through this interface using MD5 authentication.
Key ID	When you select **Simple** or **MD5** in the **Authentication** field, specify the identification number of the authentication you want to use.
Key	When you select **Simple** in the **Authentication** field, enter a password eight-character long. Characters after the eighth character will be ignored. When you select **MD5** in the **Authentication** field, enter a password 16-character long.
Cost	The interface cost is used for calculating the routing table. Enter a number between 0 and 65535.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to start configuring the above fields again.

26.6 Configuring OSPF Virtual Links

In the **OSPF Configuration** screen, click **Virtual Link** to display the screen as shown next.

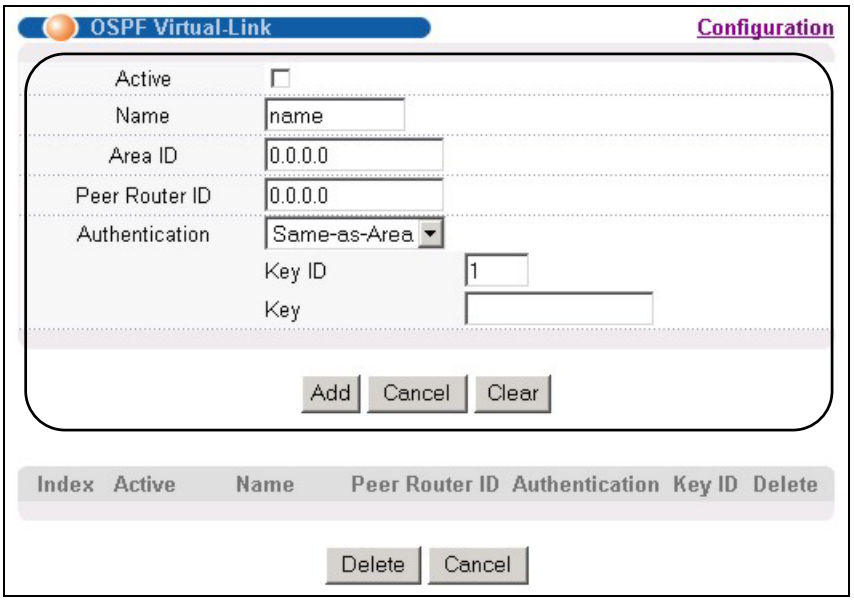


Figure 26-8 OSPF Virtual Link

The following table describes the related labels in this screen.

Table 26-8 OSPF Virtual Link

LABEL	DESCRIPTION
Active	Select this option to enable this virtual link.
Name	Enter a descriptive name for this virtual link.
AreaID	Enter the domain of a transit area in dotted decimal notation.
Peer Router ID	Enter the IP address of a peer border router.
Authentication	**Virtual interface(s) must use the same authentication method within the same area.** Select an authentication method. Choices are **Same-as-Area**, **None** (default), **Simple** and **MD5**. To exchange OSPF packets with peer border router, you must set the authentication method and/or password the same as the peer border router. Select **Same-as-Area** to use the same authentication method within the area and set the related fields when necessary. Select **None** to disable authentication. This is the default setting. Select **Simple** to authenticate OSPF packets transmitted through this interface using a simple password. Select **MD5** to authenticate OSPF packets transmitted through this interface using MD5 authentication.
Key ID	When you select **MD5** in the **Authentication** field, specify the identification number of the authenticate you want to use.
Key	When you select **Simple** in the **Authentication** field, enter a password eight-character long. When you select **MD5** in the **Authentication** field, enter a password 16-character long.
Add	Click **Add** to apply the changes.

Table 26-8 OSPF Virtual Link

LABEL	DESCRIPTION
Cancel	Click **Cancel** to start configuring the above fields again.
Clear	Click **Clear** to set the above fields back to the factory defaults.

26.6.1 Viewing Virtual Links

To view a list of virtual links you have created, scroll down to the bottom of the **OSPF Virtual Link** screen.

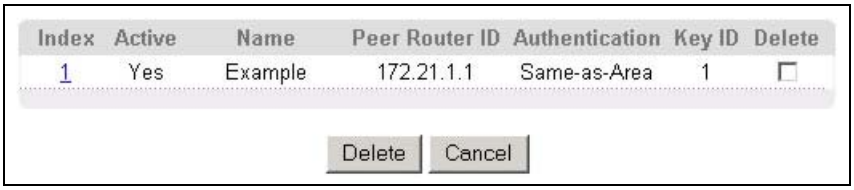


Figure 26-9 OSPF Virtual Link: Summary Table

The following table describes the related labels in this screen.

Table 26-9 OSPF Virtual Link: Summary Table

LABEL	DESCRIPTION
Index	This field displays an index number of an entry.
Active	This field displays whether a virtual link is enabled (**Yes**) or disabled (**No**).
Name	This field displays a descriptive name of a virtual link.
Peer Router-ID	This field displays the IP address of a peer border router.
Authentication	This field displays the authentication method used (**Same-as-Area**, **None**, **Simple** or **MD5**).
Key ID	When the **Authentication** field displays **MD5**, this field displays the identification number of the key used.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

Part VI

Management

This part describes the Management screens.

Chapter 27 Maintenance

This chapter explains how to configure the maintenance screens. The links on the upper right of the Maintenance screen lead to different screens that let you maintain the firmware and configuration files.

27.1 Maintenance

Click **Management**, **Maintenance** in the navigation panel to open the following screen.

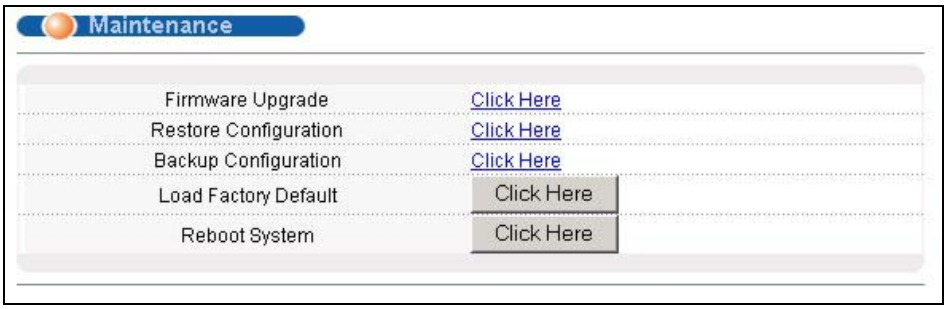


Figure 27-1 Maintenance

27.2 Firmware Upgrade

Make sure you have downloaded (and unzipped) the correct model firmware and version to your computer before uploading to the device.

Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

From the **Maintenance** screen, display the **Firmware Upgrade** screen as shown next.

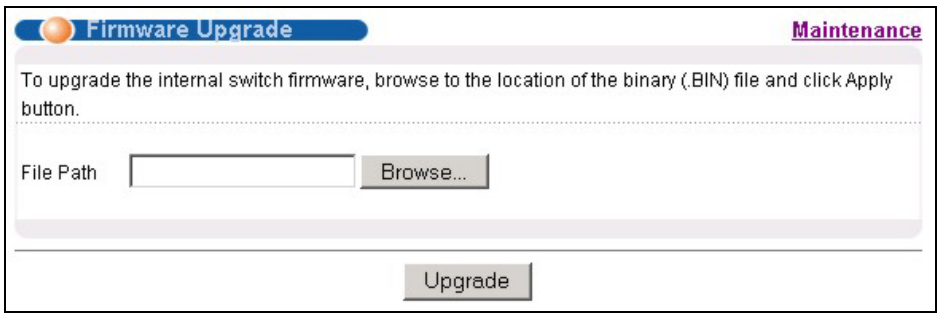


Figure 27-2 Firmware Upgrade

Type the path and file name of the firmware file you wish to upload to the switch in the **File Path** text box or click **Browse** to locate it. After you have specified the file, click **Upgrade**.

After the firmware upgrade process is complete, see the **System Info** screen to verify your current firmware version number.

27.3 Restore a Configuration File

Restore a previously saved configuration from your computer to the switch using the **Restore Configuration** screen.

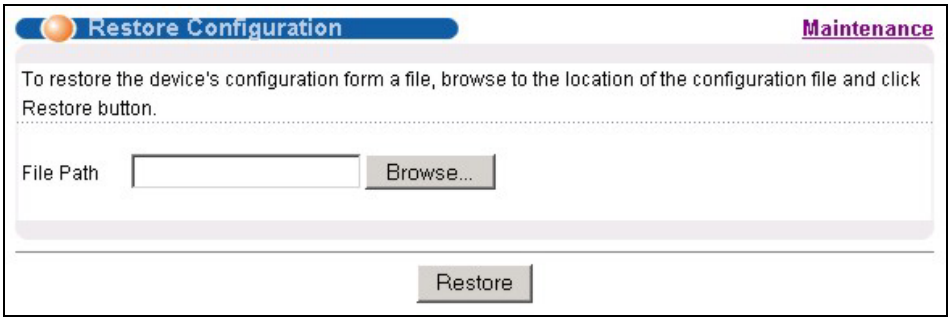


Figure 27-3 Restore Configuration

Type the path and file name of the configuration file you wish to restore in the **File Path** text box or click **Browse** to display the **Choose File** screen (below) from which you can locate it. After you have specified the file, click **Restore**. "rom-0" is the name of the configuration file on the switch, so your backup configuration file is automatically renamed when you restore using this screen.

27.4 Backing Up a Configuration File

Backing up your switch configurations allows you to create various “snap shots” of your device from which you may restore at a later date.

Back up your current switch configuration to a computer using the **Backup Configuration** screen.

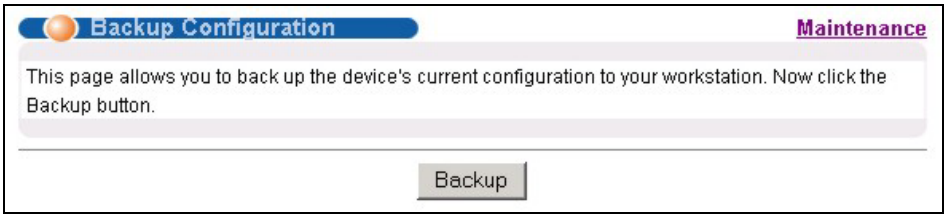


Figure 27-4 Backup Configuration

Follow the steps below to back up the current switch configuration to your computer in this screen.

Step 1. Click **Backup**.

Step 2. Click **Save** to display the **Save As** screen.

Step 3. Choose a location to save the file on your computer from the **Save in** drop-down list box and type a descriptive name for it in the **File name** list box. Click **Save** to save the configuration file to your computer.

27.5 Load Factory Defaults

Follow the steps below to reset the ES-4024 back to the factory defaults.

Step 1. In the **Maintenance** screen, click the **Click Here** button next to **Load Factory Defaults** to clear all switch configuration information you configured and return to the factory defaults. The following message appears.

Figure 27-5 Load Factory Default: Conformation

Step 2. Click **OK** to display the screen shown next.

Figure 27-6 Load Factory Default: Start

Step 3. Click **OK** to begin resetting all switch configurations to the factory defaults and then wait for the switch to restart. This takes up to two minutes. If you want to access the switch web configurator again, you may need to change the IP address of your computer to be in the same subnet as that of the default switch IP address (192.168.1.1).

27.6 Reboot System

Reboot System allows you to restart the switch without physically turning the power off. Follow the steps below to reboot the ES-4024.

Step 1. In the **Maintenance** screen, click the **Click Here** button next to **Reboot System** to display the next screen.

Figure 27-7 Reboot System: Confirmation

Step 2. Click **OK** to display the screen shown next.

Figure 27-8 Reboot System: Start

Step 3. Click **OK** again and then wait for the switch to restart. This takes up to two minutes. This does not affect the switch's configuration.

27.7 FTP Command Line

This section shows some examples of uploading to or downloading files from the switch using FTP commands. First, understand the filename conventions.

27.7.1 Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the screens such as password, switch setup, IP Setup, etc. It arrives from ZyXEL with a "rom" filename extension. Once you have customized the switch's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the "ras" file) is the system firmware and has a "bin" filename extension.

Table 27-1 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	Rom-0	*.rom	This is the configuration filename on the switch. Uploading the rom-0 file replaces the entire ROM file system, including your switch configurations, system-related data (including the default password), the error log and the trace log.
Firmware	Ras	*.bin	This is the generic name for the ZyNOS firmware on the switch.

Example FTP Commands

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file " firmware.bin" to the switch .

```
ftp> get rom-0 config.cfg
```

This is a sample FTP session saving the current configuration to a file called "config.cfg" on your computer.

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the switch only recognizes "rom-0" and "ras". Be sure you keep unaltered copies of both files for later use.

Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

27.7.2 FTP Command Line Procedure

Step 1. Launch the FTP client on your computer.

Step 2. Enter "open", followed by a space and the IP address of your switch.

Step 3. Press [ENTER] when prompted for a username.

Step 4. Enter your password as requested (the default is "1234").

Step 5. Enter "bin" to set transfer mode to binary.

Step 6. Use "put" to transfer files from the computer to the switch, for example, "put firmware.bin ras" transfers the firmware on your computer (firmware.bin) to the switch and renames it "ras". Similarly, "put config.rom rom-0" transfers the configuration file on your computer (config.rom) to the switch and renames it "rom-0". Likewise "get rom-0 config.rom" transfers the configuration file on the switch to your computer and renames it "config.rom." See earlier in this chapter for more information on filename conventions.

Step 7. Enter "quit" to exit the ftp prompt.

27.7.3 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 27-2 General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode. Configuration and firmware files should be transferred in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

27.7.4 FTP over WAN Restrictions

FTP over WAN will not work when:

- Telnet service is disabled in **Secured Client Sets**.
- The IP address(es) in the **Secured Client Sets** menu does not match the client IP address. If it does not match, the switch will disconnect the Telnet session immediately.

Chapter 28 Diagnostic

This chapter explains the Diagnostic screens.

28.1 Diagnostic

Click **Management**, **Diagnostic** in the navigation panel to open this screen. Use this screen to check system logs, reset the system or ping IP addresses.

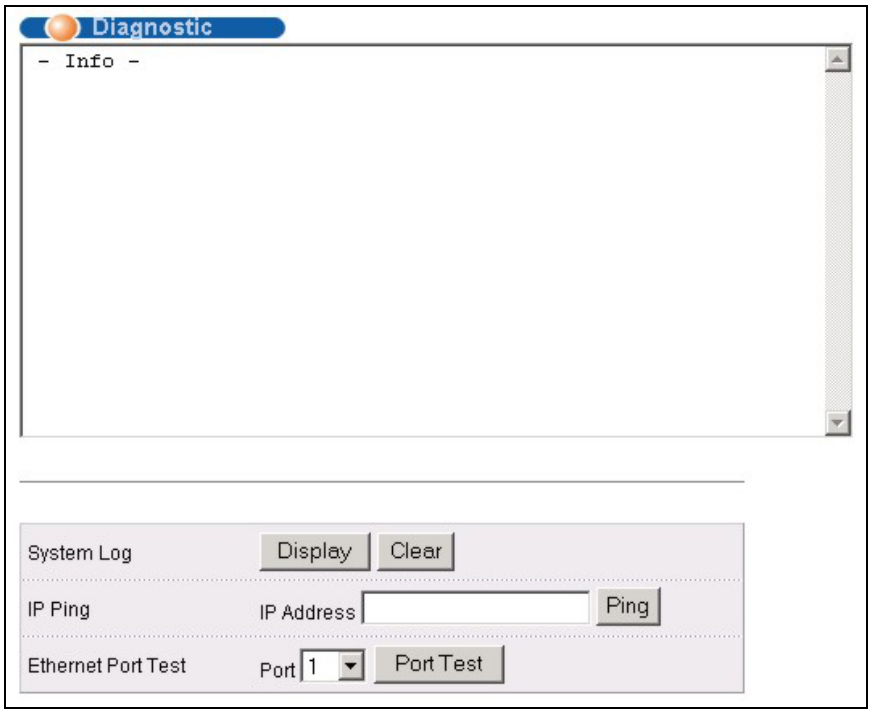


Figure 28-1 Diagnostic

The following table describes the labels in this screen.

Table 28-1 Diagnostic

LABEL	DESCRIPTION
System Log	Click **Display** to display a log of events in the multi-line text box. Click **Clear** to empty the text box and reset the syslog entry.
IP Ping	Type the IP address of a device that you want to ping in order to test a connection. Click **Ping** to have the switch ping the IP address (in the field to the left).
Ethernet Port Test	From the **Port** drop-down list box, select a port number and click **Port Test** to perform internal loopback test.

Chapter 29
Cluster Management

This chapter introduces cluster management.

29.1 Introduction to Cluster Management

Cluster Management allows you to manage switches through one switch, called the cluster manager. The switches must be directly connected and be in the same VLAN group so as to be able to communicate with one another.

Table 29-1 ZyXEL Clustering Management Specifications

Maximum number of cluster members	24
Cluster Member Models	Must be compatible with ZyXEL cluster management implementation.
Cluster Manager	The switch through which you manage the cluster member switches.
Cluster Members	The switches being managed by the cluster manager switch.

In the following example, switch A in the basement is the cluster manager and the other switches on the upper floors of the building are cluster members.

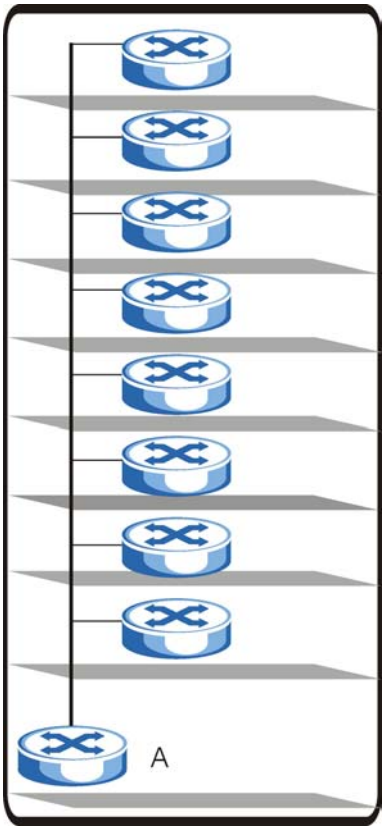


Figure 29-1 Clustering Application Example

29.2 Cluster Management Status

Click **Management**, **Cluster Management** in the navigation panel to display the following screen.

A cluster can only have one manager.

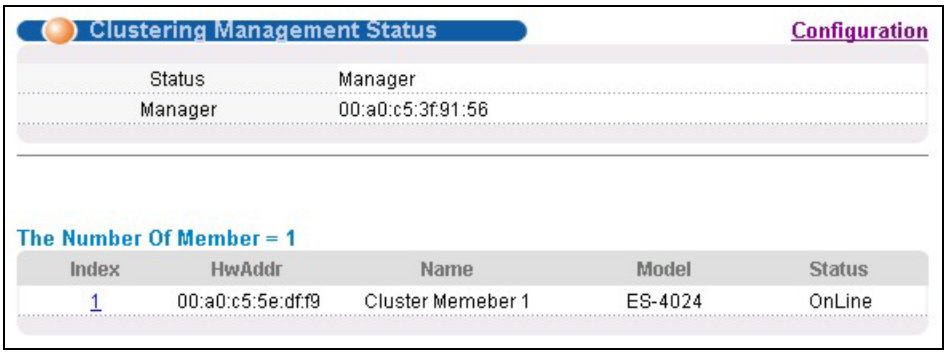


Figure 29-2 Cluster Management: Status

The following table describes the labels in this screen.

Table 29-2 Cluster Management Status

LABEL	DESCRIPTION
Status	This field displays the role of this switch within the cluster. o **Manager** o **Member** (you see this if you access this screen in the cluster member switch directly and not via the cluster manager) o **None** (neither a manager nor a member of a cluster)
Manager	This field displays the cluster manager switch's hardware MAC address.
The Number of Member	This field displays the number of switches that make up this cluster. The following fields describe the cluster member switches.
Index	You can manage cluster member switches via the cluster manager switch. Each number in the **Index** column is a hyperlink leading to the cluster member switch's web configurator (see *Figure 29-3*).
HwAddr	This is the cluster member switch's hardware MAC address.
Name	This is the cluster member switch's **System Name**.
Model	This field displays the model name.
Status	This field displays: o **Online** (the cluster member switch is accessible) o **Error** (for example the cluster member switch password was changed or the switch was set as the manager and so left the member list, etc.) o **Offline** (the switch is disconnected - **Offline** shows approximately 1.5 minutes after the link between cluster member and manager goes down)

29.2.1 Cluster Member Switch Management

Go to the **Clustering Management Status** screen of the cluster manager switch and then select an **Index** hyperlink from the list of members to go to that cluster member switch's web configurator home page. This cluster member web configurator home page and the home page that you'd see if you accessed it directly are different.

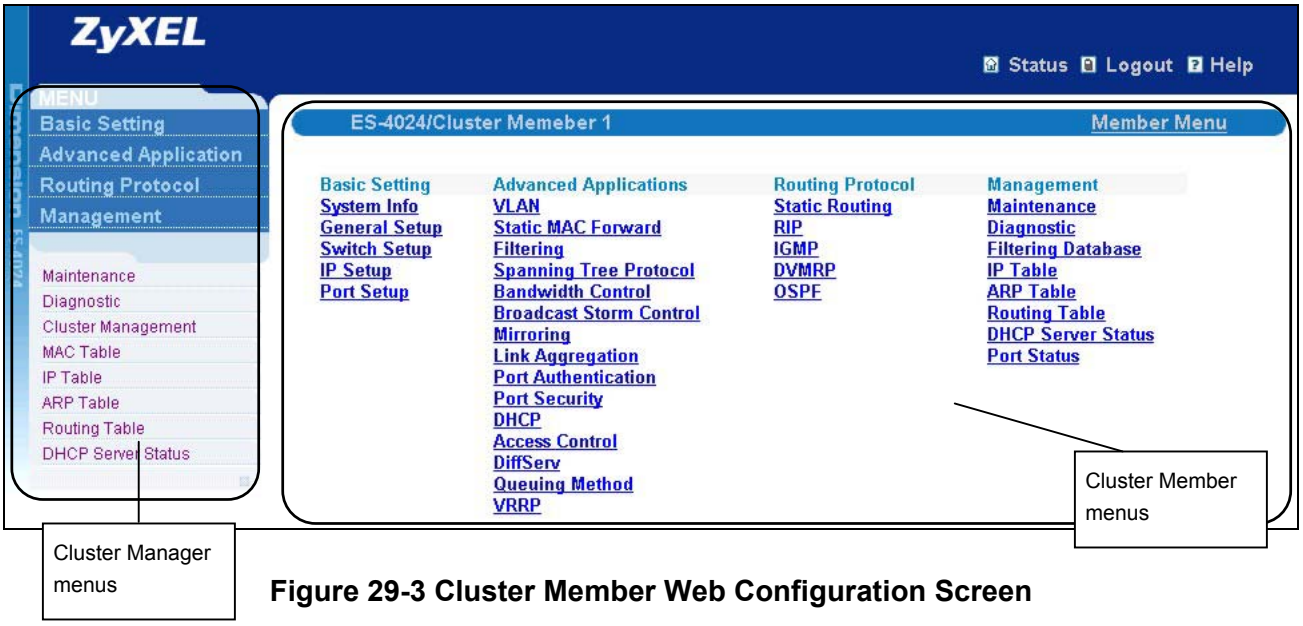


Figure 29-3 Cluster Member Web Configuration Screen

Uploading Firmware to a Cluster Member Switch

You can use FTP to upload firmware to a cluster member switch through the cluster manager switch as shown in the following example.

```
ftp 192.168.1.1
Connected to 192.168.1.1.
220 ES-4024 FTP version 1.0 ready at Sat Jan 01 00:11:33 2000
User (192.168.1.1:(none)):
331 Enter PASS command
Password:
230 Logged in
ftp> ls
200 Port command okay
150 Opening data connection for LIST
--w--w--w-   1 owner    group         1810050 Jul 01 12:00 ras
-rw-rw-rw-   1 owner    group          262144 Jul 01 12:00 rom-0
--w--w--w-   1 owner    group               0 Jul 01 12:00 fw-00-a0-c5-5e-df-f9
-rw-rw-rw-   1 owner    group               0 Jul 01 12:00 config-00-a0-c5-5e-df-f9
-f9
226 File sent OK
ftp: 296 bytes received in 0.00Seconds 296000.00Kbytes/sec.
ftp> bin
200 Type I OK
ftp> put 350du1b2.rom config-00-a0-c5-5e-df-f9
200 Port command okay
150 Opening data connection for STOR config-00-a0-c5-5e-df-f9
226 File received OK
ftp: 262144 bytes sent in 0.63Seconds 415.44Kbytes/sec.
ftp>
```

Figure 29-4 Example: Uploading Firmware to a Cluster Member Switch

The following table explains some of the FTP parameters.

Table 29-3 FTP Upload to Cluster Member Example

FTP PARAMETER	DESCRIPTION
`User`	Press <Enter>
`Password`	The web configurator password default is 1234.
`ls`	Enter this command to list the name of cluster member switch's firmware and configuration file.
`350du1b2.bin`	The name of the firmware file you want to upload to the cluster member switch.
`fw-00-a0-c5-5e-df-f9`	The cluster member switch's firmware name as seen in the cluster manager switch.
`config-00-a0-c5-5e-df-f9`	The cluster member switch's configuration file name as seen in the cluster manager switch.

29.3 Configuring Cluster Management

Click **Configuration** from the **Cluster Management** screen to display the next screen.

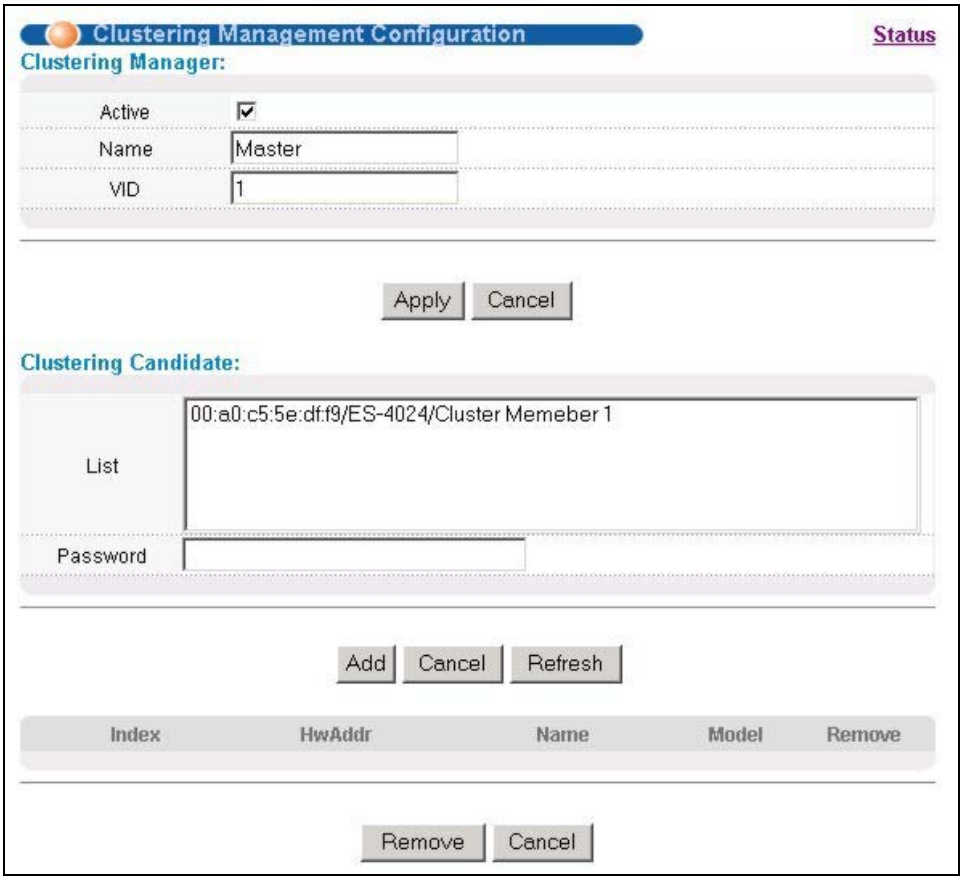


Figure 29-5 Clustering Management Configuration

The following table describes the labels in this screen.

Table 29-4 Clustering Management Configuration

LABEL	DESCRIPTION
Clustering Manager	
Active	Select **Active** to have this switch become the cluster manager switch. A cluster can only have one manager. Other (directly connected) switches that are set to be cluster managers will not be visible in the **Clustering Candidates** list. If a switch that was previously a cluster member is later set to become a cluster manager, then its **Status** is displayed as **Error** in the **Cluster Management Status** screen and a warning icon ( ) appears in the member summary list below.
Name	Type a name to identify the **Clustering Manager.** You may use up to 20 printable characters (no spaces are allowed).
VID	This is the Management VLAN ID and is only applicable if the switch is set to **802.1Q** VLAN. All switches must be in the same management VLAN group to belong to the same cluster. Switches that are not in the same management VLAN group are not visible in the **Clustering Candidates** list. This field is ignored if the **Clustering Manager** is using **Port-based** VLAN.
Apply	Click **Apply** to save these changes to the switch.

Table 29-4 Clustering Management Configuration

LABEL	DESCRIPTION
Cancel	Click **Cancel** to begin configuring this part of the screen afresh.
Clustering Candidate	The following fields relate to the switches that are potential cluster members.
List	A list of suitable candidates found by auto-discovery is shown here. The switches must be directly connected. Directly connected switches that are set to be cluster managers will not be visible in the **Clustering Candidate** list. Switches that are not in the same management VLAN group will not be visible in the **Clustering Candidate** list.
Password	Each cluster member's password is its web configurator password. Select a member in the **Clustering Candidate** list and then enter its web configurator password. If that switch administrator changes the web configurator password afterwards, then it cannot be managed from the **Cluster Manager**. Its **Status** is displayed as **Error** in the **Cluster Management Status** screen and a warning icon ( ) appears in the member summary list below. If multiple devices have the same password then hold [SHIFT] and click those switches to select them. Then enter their common web configurator password.
Add	Click **Add** to save this part of the screen to the switch.
Cancel	Click **Cancel** to begin configuring this part of the screen afresh.
Refresh	Click **Refresh** to perform auto-discovery again to list potential cluster members.
The next summary table shows the information for the clustering members configured.	
Index	This is the index number of a cluster member switch.
HwAddr	This is the cluster member switch's hardware MAC address.
Name	This is the cluster member switch's **System Name**.
Model	This is the cluster member switch's model name.
Remove	Select this checkbox and then click the **Remove** button to remove a cluster member switch from the cluster.
Cancel	Click **Cancel** to begin configuring this part of the screen afresh.

Chapter 30 MAC Table

This chapter introduces the MAC Table screen.

30.1 Introduction to MAC Table

The **MAC Table** screen (a MAC table is also known as a filtering database) shows how frames are forwarded or filtered across the switch's ports. It shows what device MAC address, belonging to what VLAN group (if any) is forwarded to which port(s) and whether the MAC address is dynamic (learned by the switch) or static (manually entered in the **Static MAC Forwarding** screen).

The switch uses the MAC table to determine how to forward frames. See the following figure.

1. The switch examines a received frame and learns the port on which this source MAC address came.
2. The switch checks to see if the frame's destination MAC address matches a source MAC address already learned in the MAC table.

- If the switch has already learned the port for this MAC address, then it forwards the frame to that port.
- If the switch has not already learned the port for this MAC address, then the frame is flooded to all ports. Too much port flooding leads to network congestion.
- If the switch has already learned the port for this MAC address, but the destination port is the same as the port it came in on, then it filters the frame.

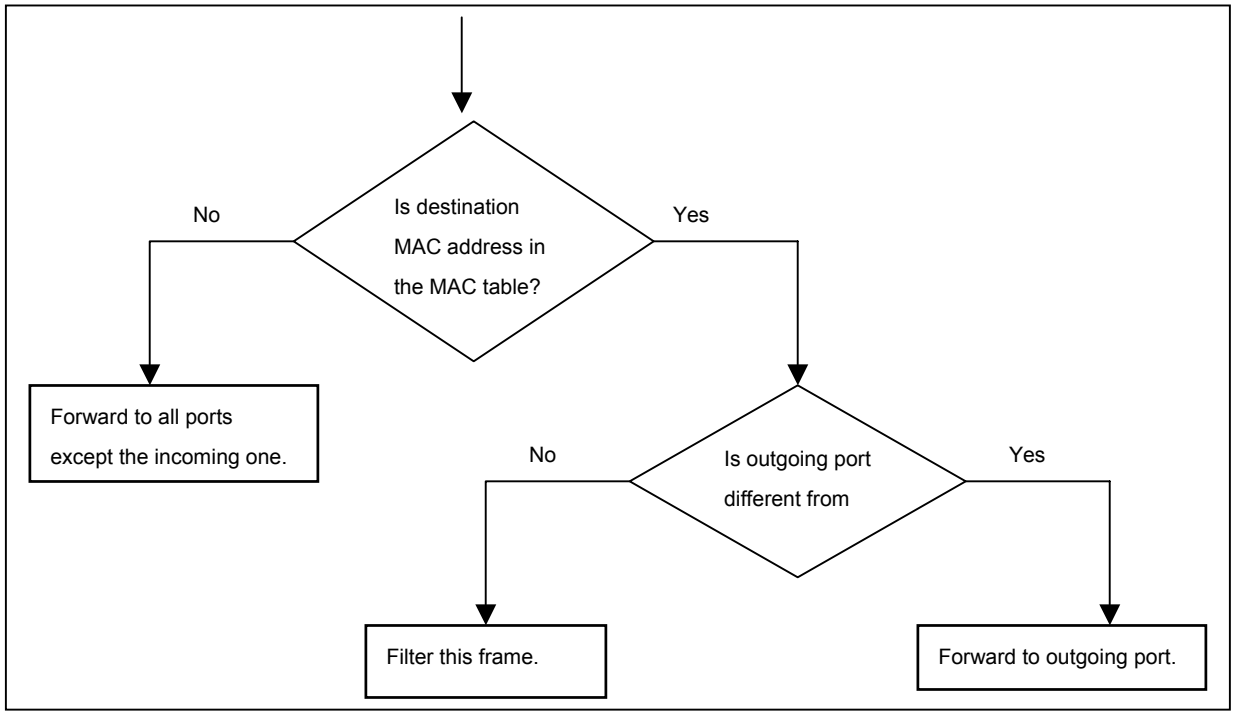


Figure 30-1 MAC Table Flowchart

30.2 Viewing the MAC Table

Click **Management**, **MAC Table** in the navigation panel to display the following screen. The MAC table can hold up to 16K entries.

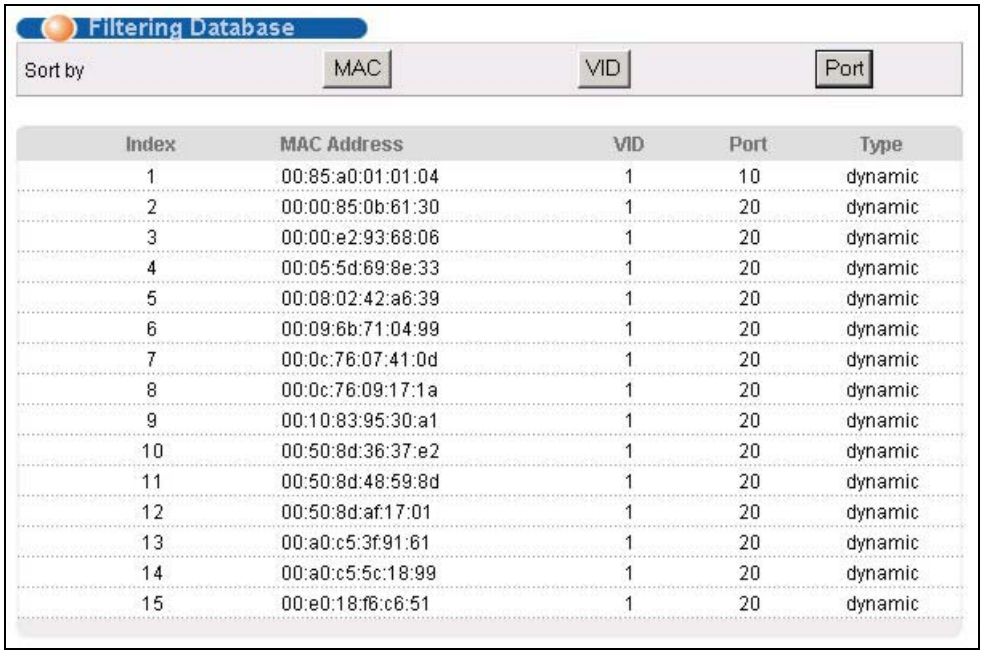


Figure 30-2 Filtering Database

The following table describes the labels in this screen.

Table 30-1 Filtering Database

LABEL	DESCRIPTION
Sort by	Click one of the following buttons to display and arrange the data according to that button type. The information is then displayed in the summary table below.
MAC	Click this button to display and arrange the data according to MAC address.
VID	Click this button to display and arrange the data according to VLAN group.
Port	Click this button to display and arrange the data according to port number.
Index	This is the incoming frame index number.
MAC Address	This is the MAC address of the device from which this incoming frame came.
VID	This is the VLAN group to which this frame belongs.
Port	This is the port from which the above MAC address was learned.
Type	This shows whether the MAC address is **dynamic** (learned by the switch) or **static** (manually entered in the **Static MAC Forwarding** screen).

Chapter 31
IP Table

This chapter introduces the IP table.

31.1 Introduction to IP Table

The **IP Table** screen shows how packets are forwarded or filtered across the switch's ports. It shows what device IP address, belonging to what VLAN group (if any) is forwarded to which port(s) and whether the IP address is dynamic (learned by the switch) or static (belonging to the switch).

The switch uses the IP table to determine how to forward packets. See the following figure.

3. The switch examines a received packet and learns the port on which this source IP address came.
4. The switch checks to see if the packet's destination IP address matches a source IP address already learned in the IP table.

- If the switch has already learned the port for this IP address, then it forwards the packet to that port.
- If the switch has not already learned the port for this IP address, then the packet is flooded to all ports. Too much port flooding leads to network congestion.
- If the switch has already learned the port for this IP address, but the destination port is the same as the port it came in on, then it filters the packet.

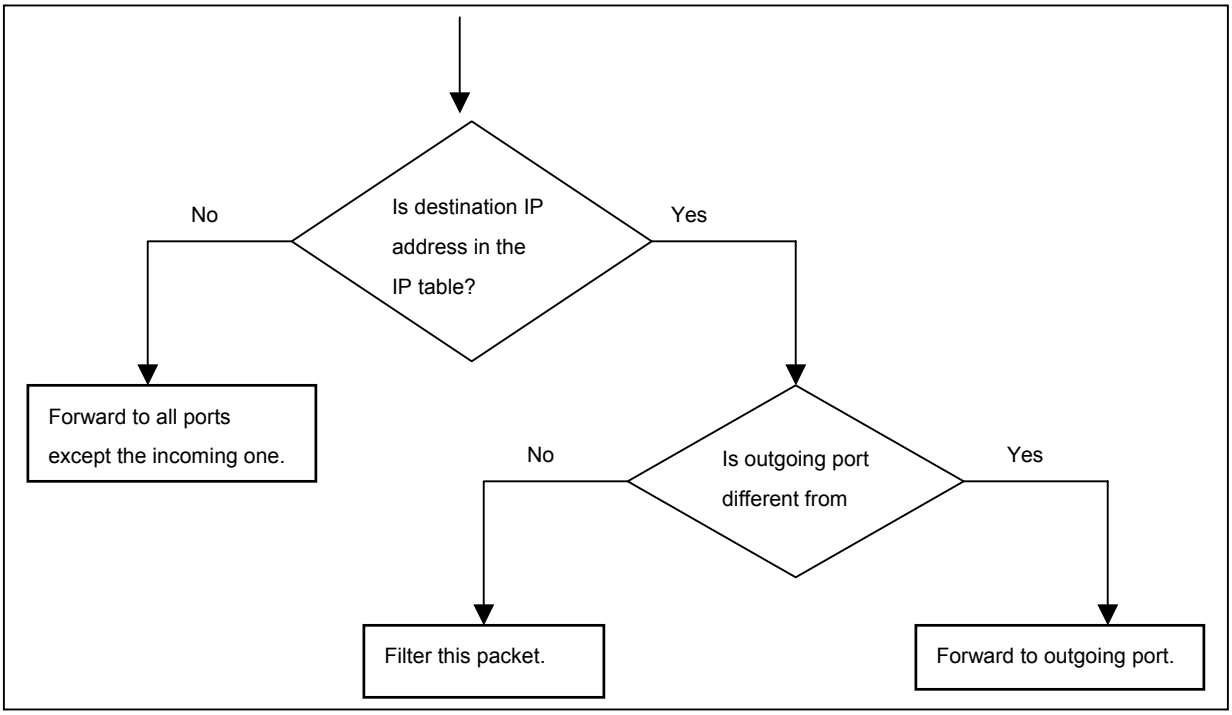


Figure 31-1 IP Table Flowchart

31.2Viewing the IP Table

Click **Management**, **IP Table** in the navigation panel to display the following screen. The IP table can hold up to 16K entries.

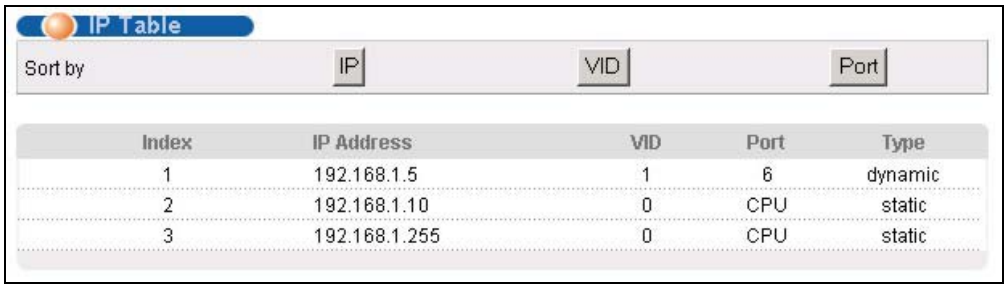


Figure 31-2 Management: IP Table

The following table describes the labels in this screen.

Table 31-1 Management: IP Table

LABEL	DESCRIPTION
Sort by	Click one of the following buttons to display and arrange the data according to that button type. The information is then displayed in the summary table below.
IP	Click this button to display and arrange the data according to IP address.
VID	Click this button to display and arrange the data according to VLAN group.
Port	Click this button to display and arrange the data according to port number.
Index	This field displays the index number.
IP Address	This is the IP address of the device from which the incoming packets came.
VID	This is the VLAN group to which the packet belongs.
Port	This is the port from which the above IP address was learned. This field displays **CPU** to indicate the IP address belongs to the switch.
Type	This shows whether the IP address is **dynamic** (learned by the switch) or **static** (belonging to the switch).

Chapter 32
ARP Table

This chapter introduces ARP Table.

32.1 Introduction to ARP Table

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network.

An IP (version 4) address is 32 bits long. In an Ethernet LAN, MAC addresses are 48 bits long. The ARP Table maintains an association between each MAC address and its corresponding IP address.

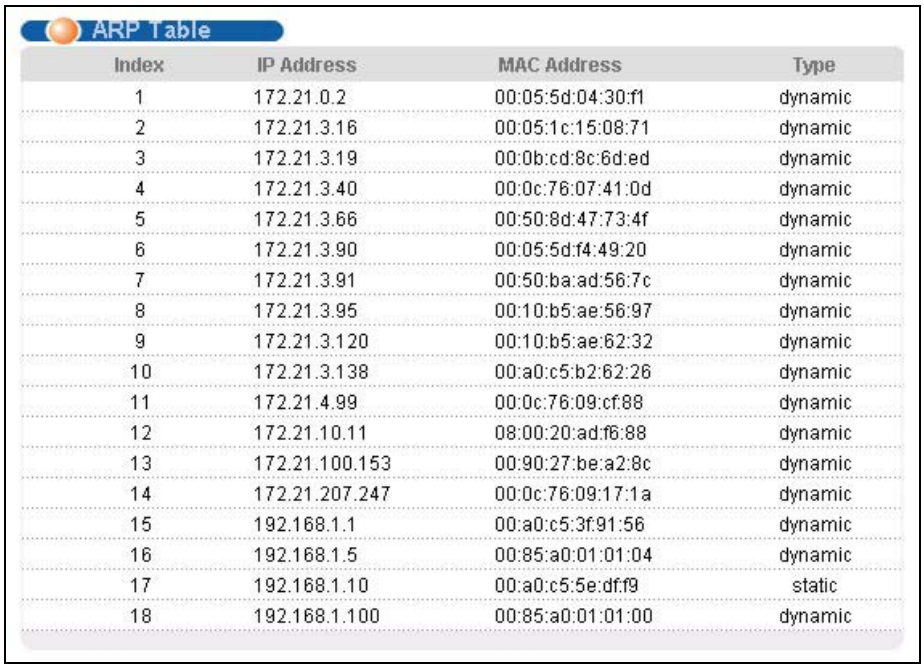
32.1.1 How ARP Works

When an incoming packet destined for a host device on a local area network arrives at the switch, the switch's ARP program looks in the ARP Table and, if it finds the address, sends it to the device.

If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The switch fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the switch puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP Table for future reference and then sends the packet to the MAC address that replied.

32.2 Viewing ARP Table

Click **Management**, **ARP Table** in the navigation panel to open the following screen. The ARP table can hold up to 500 entries.



ARP Table

Index	IP Address	MAC Address	Type
1	172.21.0.2	00:05:5d:04:30:f1	dynamic
2	172.21.3.16	00:05:1c:15:08:71	dynamic
3	172.21.3.19	00:0b:cd:8c:6d:ed	dynamic
4	172.21.3.40	00:0c:76:07:41:0d	dynamic
5	172.21.3.66	00:50:8d:47:73:4f	dynamic
6	172.21.3.90	00:05:5d:f4:49:20	dynamic
7	172.21.3.91	00:50:ba:ad:56:7c	dynamic
8	172.21.3.95	00:10:b5:ae:56:97	dynamic
9	172.21.3.120	00:10:b5:ae:62:32	dynamic
10	172.21.3.138	00:a0:c5:b2:62:26	dynamic
11	172.21.4.99	00:0c:76:09:cf:88	dynamic
12	172.21.10.11	08:00:20:ad:f6:88	dynamic
13	172.21.100.153	00:90:27:be:a2:8c	dynamic
14	172.21.207.247	00:0c:76:09:17:1a	dynamic
15	192.168.1.1	00:a0:c5:3f:91:56	dynamic
16	192.168.1.5	00:85:a0:01:01:04	dynamic
17	192.168.1.10	00:a0:c5:5e:df:f9	static
18	192.168.1.100	00:85:a0:01:01:00	dynamic

Figure 32-1 ARP Table

The following table describes the labels in this screen.

Table 32-1 ARP Table

LABEL	DESCRIPTION
Index	This is the ARP Table entry number.
IP Address	This is the learned IP address of a device connected to a switch port with corresponding MAC address below.
MAC Address	This is the MAC address of the device with corresponding IP address above.
Type	This shows whether the MAC address is dynamic (learned by the switch) or static (manually entered in the **Static MAC Forwarding** screen).

Chapter 33 Routing Table

This chapter introduces the routing table.

33.1 About the Routing Table

The routing table contains the route information to the network(s) that the ES can reach. The ES automatically updates the routing table with the RIP information received from other Ethernet devices.

33.2 Viewing the Routing Table

Click **Management**, **Routing Table** in the navigation panel to display the screen as shown.

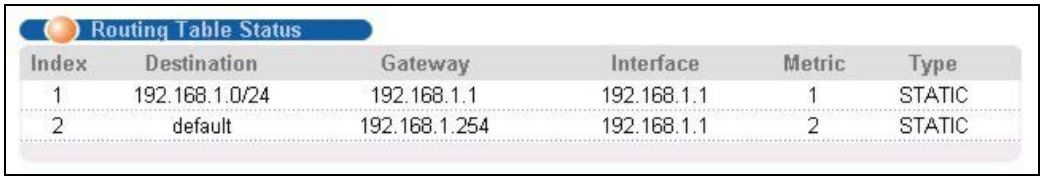


Figure 33-1 Management: Routing Table Status

The following table describes the labels in this screen.

Table 33-1 Management: Routing Table Status

LABEL	DESCRIPTION
Index	This field displays the index number.
Destination	This field displays the destination IP routing domain.
Gateway	This field displays the IP address of the gateway device.
Metric	This field displays the cost of the route.
Type	This field displays the method used to learn the route.

Chapter 34
DHCP Server Status

This chapter shows you how to view the DHCP server status.

34.1 About DHCP Server Status

The **DHCP Server Status** screen displays the summary table about the DHCP server(s) you configured in the **DHCP** screen. You can also view detail DHCP server information in the **Server Status Detail** screen.

34.2 Displaying DHCP Server Status

Click **Management**, **DHCP Server Status** in the navigation panel to display the screen as shown.

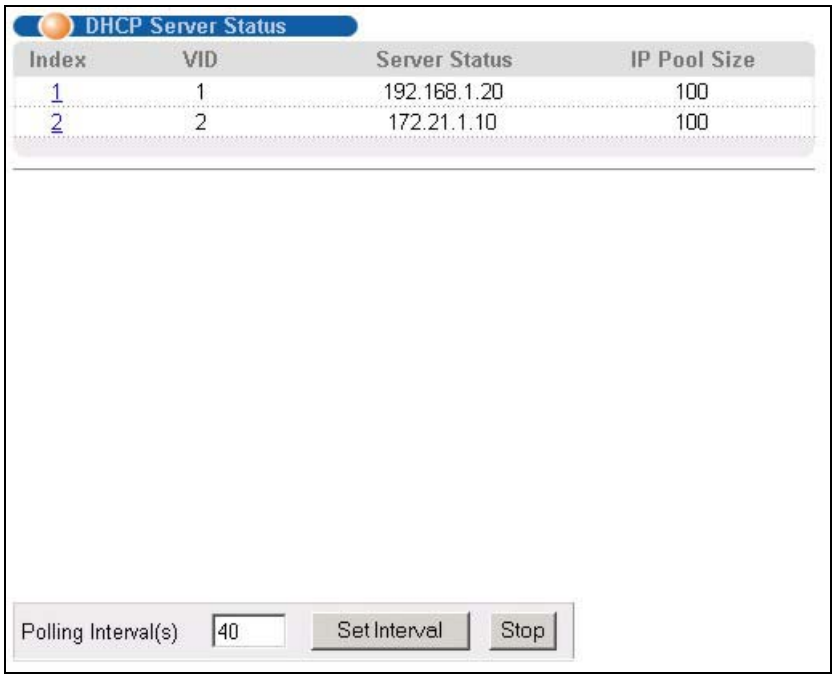


Figure 34-1 Management: DHCP Server Status

The following table describes the labels in this screen.

Table 34-1 Management: DHCP Server Status

LABEL	DESCRIPTION
Index	This field displays the index number.
VID	This field displays the ID of the VLAN to which the DHCP server belongs. Click on a VID to display detail server information (refer to *Section 34.3*).
Server Status	This field displays the starting IP address of the client address pool.
IP Pool Size	This field displays the count of the DHCP client IP address pool.

Table 34-1 Management: DHCP Server Status

LABEL	DESCRIPTION
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt polling statistics.

34.3 Displaying Detail DHCP Server Information

To view detail DHCP server information (such as client addresses and IP address lease time), click a VID in the **DHCP Server Status** screen.

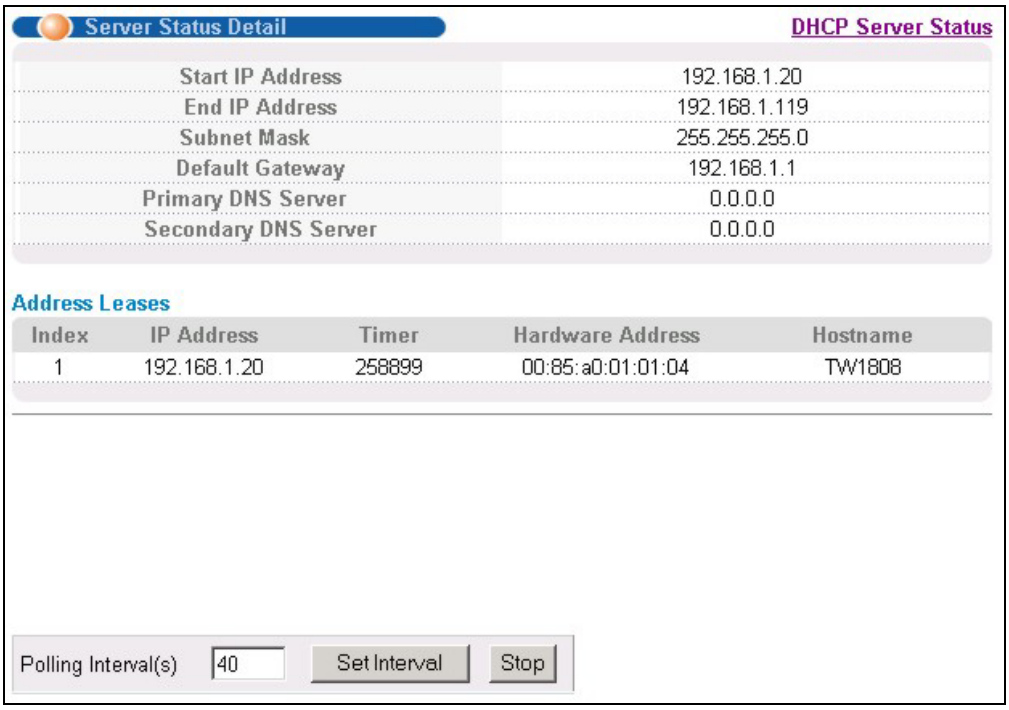


Figure 34-2 DHCP Server Status Detail

The following table describes the labels in this screen.

Table 34-2 DHCP Server Status Detail

LABEL	DESCRIPTION
Start IP Address	The field displays the first of the contiguous addresses in the IP address pool
End IP Address	The field displays the last of the contiguous addresses in the IP address pool
Subnet Mask	This field displays the subnet mask in dotted decimal notation.
Default Gateway	This field displays the IP address (in dotted decimal notation) of the default gateway device.
Primary DNS Server	This field displays the IP address (in dotted decimal notation) of the primary DNS server.
Secondary DNS Server	This field displays the IP address (in dotted decimal notation) of the secondary DNS server.
Address Leases	

Table 34-2 DHCP Server Status Detail

LABEL	DESCRIPTION
Index	This field displays the index number.
IP Address	This field displays the IP address assigned to a DHCP client device.
Timer	This field displays the time (in seconds) the DHCP client is allowed to use the assigned IP address.
Hardware Address	This field displays the MAC address (in hexadecimal notation) of the DHCP client device.
Hostname	This field displays the DHCP client device name.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt polling statistics.

Part VII

Commands

This part gives information on Command Line Interface (CLI) for the ES-4024.

Chapter 35
Introduction to CLI

This chapter introduces line commands and gives a summary of commands available.

35.1 Command Line Interface Overview

In addition to the web configurator, you can use line commands to configure the switch. It is recommended that you use the web configurator for everyday management of the switch and that you use line commands for advanced switch diagnosis and troubleshooting. If you have problems with your switch, customer support may request that you issue some of these commands to assist them in troubleshooting.

You can use the "config save" command to save 802.1Q, STP, Cluster and IP configuration changes to non-volatile memory (Flash). These changes are effective after you restart the switch.

However you cannot use "config save" for all other line command configurations. These are saved in volatile memory (DRAM), so are not effective after you restart the switch.

35.1.1 Accessing the Command Line Interface

There are two ways to access the command line interface on the ES-4024:

- Telnet to the switch
- Connect a computer to the console port and use a terminal emulation software configured to the following parameters:
  - VT100 terminal emulation
  - 9600 bps
  - No parity, 8 data bits, 1 stop bit
  - No flow control

35.1.2 Command Conventions

The system uses a one-level command structure. You must type the full command every time, as follows.

```
192.168.1.1> <command>
```

For instance, the following example shows how to enable GVRP.

```
192.168.1.1> sys sw gvrp enable
```

The conventions for typing in most CI commands are shown next.

```
command <interface|device> subcommand [parameter]
command subcommand [parameter]
```

35.1.3 Command Syntax Conventions

1. Command keywords are in `courier new` font.
2. The | symbol means “or”.
3. Required fields in a command are enclosed in angle brackets <>. Use the following command to turn the system monitor on or off.

   ```
   sys monitor enable <on/off>
   ```

4. Optional fields in a command are enclosed in square brackets [], for example, year, month and day are optional in the following command. This command just displays the date if you don’t specify the year, month and day parameters.

   ```
   sys date [year month day]
   ```

5. Commands can be abbreviated to the smallest unique string that differentiates the command. For example the “system date” command could be abbreviated to “s d”.

Type all commands as displayed on the screen.

35.1.4 Getting Help

Type “help” or “?” to display a list of valid commands or type a command followed by “help” or “?” to display a list of associated subcommands.

The following figure shows a sample help information.

```
ES-4024> ?
Valid commands are:
sys             exit            ip

ES-4024> sys view ?
Usage: view <filename>
```

Figure 35-1 CLI Help: Sample Output

35.2 Command Summary

The following tables are summaries of the commands available in the ES-4024 together with a brief description of each command. See the related section in the *User’s Guide* for more background information.

35.2.1 sys Commands

Table 35-1 CLI Command Summary: sys

COMMAND			DESCRIPTION
sys			

Table 35-1 CLI Command Summary: sys

COMMAND			DESCRIPTION
	adjtime		Retrieves the date and time from the time server specified in the web configurator.
	countrycode	<country code>	Sets or displays the firmware country code.
	cpld	revision	Show the CPLD (Complex Programmable Logic Device) hardware revision.
		alarm <on|off>	Turn the ALARM LED on/off manually
		status	Counter of CPLD faults
	cpu	display	Displays the CPU's utilization.
	date	[year month day]	Sets or displays the system's current date.
	domainname	[domain name]	Sets or displays the system domain name.
	edit	edit filename	Edits the system preset text file such as autoexec.net.
	feature		Displays a list of the device's major features.
	hostname	[hostname]	Sets or displays the system name.
	log	clear	Clears the error log.
		disp	Shows the error log.
		online [on|off]	Enables/disables the error log to be displayed on screen.
	stdio	[minute]	Sets or displays the management terminal idle timeout value.
	syslog	server	Sets syslog server IP address
		facility	Sets syslog facility
		type	Sets/displays syslog type flag
		mode	Sets syslog mode
	time	hour [min [sec]]]	Sets or displays the system time.
	trcdisp	parse, brief, disp	Sets the level of detail that should be displayed. Use "parse" to display the most detail and "disp" to display the least.
	trclog	switch [on|off]	Enables/disables the system trace log or shows whether it's on or off.
		online [on|off]	Enables/disables the trace log onscreen display (for example in the telnet management window).

Table 35-1 CLI Command Summary: sys

COMMAND			DESCRIPTION
		level [level]	Sets the level (1-10) of trace logs (1 shows the least) to display.
		type <bitmap>	Uses hexadecimal characters to set the type of trace logs to record.
		disp	Shows the trace log.
		clear	Erases the trace log.
		call	Shows call events.
		encapmask [mask]	Shows which type of encapsulation the trace log records or sets it if you specify the encapsulation's hexadecimal character.
	trcpacket	create <entry> <size>	Creates a packet trace buffer.
		destroy	Removes the packet trace buffer.
		channel <name> [none|incoming|outgoing|bothway]	Sets the packet trace direction for a given channel.
		string [on|off]	Enables/disables the sending of a log to the trace packet buffer when configuration changes are made or displays the current setting.
		switch [on|off]	Enables/disables packet trace or displays the current setting.
		disp	Displays the trace packets.
		udp	Sends the trace packets to another system using UDP.
		udp switch [on|off]	Enables/disables the sending of the trace packets to another system using UDP or displays the current setting.
		udp addr <addr>	Sets the target IP address for sending trace packets using UDP.
		udp port <port>	Sets the UDP port (should match that of the target IP address) for sending trace packets using UDP.
		parse [[start_idx], end_idx]	Displays detailed packet details of the packet range specified.
		brief	Displays a brief listing of packet contents.
	version		Displays the RAS code and driver versions.
	view	view <filename>	Displays the specified text file.
	wdog		

Table 35-1 CLI Command Summary: sys

COMMAND			DESCRIPTION
		switch [on|off]	Turns the watchdog firmware protection feature on or off.
		cnt [value]	Sets (0-34463) or displays the current watchdog count (in 1.6 sec units).
	monitor	status	Displays the status of the hardware monitor.
		show	Displays the hardware monitor's statistics.
		vlimit <idx> <high> <low>	Sets the maximum (<high>) or minimum (<low>) voltage at the specified point (<idx>).
		tlimit <idx> <limit>	Sets the maximum (<limit>) temperature at the specified point (<idx>).
		flimit <bank> <idx> [<limit>]	Sets the maximum (<limit>) fan revs per minute (RPM) at the specified fan (<idx>) in the specified bank (<bank>). A "bank" delineates a set of fans.
		fanmask <bank> [<mask>]	Sets the fan detection mask in the specified bank (<bank>). Use the mask to disable monitoring of a fan.
		vclear	Clears the voltage statistics.
		tclear	Clears the temperature statistics.
		fclear	Clears the fan statistics.
		clear	Clears the hardware monitor statistics.
		enable [<on/off>]	Enables or disables the hardware monitor.
		test	Tests the hardware monitor chip.
	ixe2424	lbt intlbt <port|All> [count]	ixe2424 refers to the switch chip. Performs an internal loop back test on a specified port or all ports.
		lbt extlbt <port> [count]	Performs an external loop back test on a specified port or all ports.
		pktcnt <port 1-28>	Displays port statistic counter
		pktcntclear <port 1-28>	Resets port statistic counter
		port <portID> <enable | disable> <Speed> <FlowCtrl>	Port setup
		phyread <portID> [<phyAddr>]	Reads PHY register

Table 35-1 CLI Command Summary: sys

COMMAND			DESCRIPTION
		phywrite <portID> <phyAddr> <data>	Writes PHY register
		dbm mac count [port]	Displays the number of MAC addresses in L2 DBM
		dbm mac list [port]	Displays entries in L2 DBM
		dbm mac flush [port]	Flushes learned MAC addresses in the forwarding table.
		dbm mac search <MAC> <VID>	Searches the MAC/VID learnt on which port.
		dbm ip list [port]	Displays entries in L3 DBM
		dbm ip count	Displays the number of IP addresses in L3 DBM
		dbm ip flush	Flushes the IP address in L3 DBM.
		dbm ip search <IP>	Searches the IP address in L3 DBM.
		log level [0-4]	Sets the log level. Logs displayed consist of critical, error, warning, debug and informational messages in order of severity. Log level “4” displays all messages; log level “0” just displays critical messages.
		log switch on/off	Outputs messages to the console or telnet screen.
		log list	Lists all IXE log modules.
		log module <module_id> <on/off	Enables/disables log on specific IXE module
		memdump <start_addr> <length>	Displays the switch chip’s memory map for the block specified.
		wreg <addr> <value>	Writes to a register.
		rreg <addr>	Reads from a register.
		show_int_count	Displays the interrupt counter.
		clear_int_count	Resets the interrupt counter.
	socket		Displays the system socket’s ID #, type, control block address (PCB), IP address and port number of peer device connected to the socket (Remote Socket) and task control block (Owner).
	snmp	getCommunity <index> [<community>]	Sets or displays the SNMP GetRequest community.
		setCommunity <index> [<community>]	Sets or displays the SNMP SetRequest community.

Table 35-1 CLI Command Summary: sys

COMMAND			DESCRIPTION
		trustedHost <index>[<hostt>]	Sets or displays the SNMP trusted host.
		trapCommunity <index> [<community>]	Sets or displays the SNMP Trap community.
		trapDest <index>[<destination>]	Sets or displays the SNMP trap server.
		disp <index|all>	Shows SNMP settings.
	cluster	active <name> <vid>	Enables this switch as the cluster manager and assigns a cluster name and VID in which the manager belongs.
		inactive <name> <vid>	Disables cluster management.
		add <MAC addr> <password>	Adds a member switch into the cluster using its web configurator password.
		remove <MAC addr>	Remove a member switch from the cluster.
		showMember	Shows details of member switches in this cluster.
		showCandidate	Shows a list of auto-discovered potential cluster members.
		status	Shows whether this switch is a cluster member, cluster manager or neither and information about members in the cluster.
	romreset		Resets the switch back to the factory defaults.

35.2.2 sys sw Commands

The following commands are system switch commands; all are preceded with `sys sw`

Table 35-2 Command Summary: sys sw

COMMAND			DESCRIPTION
driver	config		Displays the switch NDIS settings.
	count	disp	Shows the switch NDIS level counters(CPU interface)
		clear	Clears the switch NDIS level counters(CPU interface)
garp	status		Shows the GARP timer status.

Table 35-2 Command Summary: sys sw

COMMAND			DESCRIPTION
	timer	<join timer(ms)><leave timer(ms)><leave all timer<ms>	Sets the GARP timer's Join Timer, Leave Timer and Leave All Timer.
gvrp	trace		Sets GVRP trace level.
	enable		Enables GVRP.
	disable		Disables GVRP.
qos	defpri	<port> [<0..7>]	Sets the default ingress User Priority for a port.
	map	<0..7> [<queue>]	Maps a User Priority to a Traffic Class.
	method	<port> <strict | wfq weight1 weight2 weight3 weight4 (Sum of all weight should be 100)>	Sets QoS method. For WFQ, the total sum must be 100.
vlan1q			All "sys sw vlan1q" commands relate to IEEE 802.1Q Tagged VLAN configuration. Use "config save" to save your configuration changes.
	port	status <port>	Shows a port's VLAN information.
		defaultVID <port><vid>	Sets the default VLAN ID of a port.
		accept <port> <all|tagged|untagged>	Sets the type of frames that a port accepts.
		gvrp <port> <enable|disable>	Enables/disables GVRP on the specified port.
		protocolVID <port><VID><protocol>	Sets protocol-based pvid for the specific port.
		vlanTrunking<port><enable/disable>	Activates/Deactivates VLAN trunking on a port.
	svlan	cpu <vlan id>	Sets the VLAN ID of the management VLAN (CPU).
		setentry<name><vid><port><adctl> <tagctl>	Applies a static VLAN (name, admin control tag, tag control) to a port.
		delentry <vid>	Deletes the specified (VID) static VLAN.
		active <vid>	Turns on the specified static VLAN.
		inactive <vid>	Turns off the specified static VLAN.
		list	Displays a table of static VLANs.
	vlan	list <all|vid|start_vid end_vid>	Shows the specified IEEE 802.1Q Tagged VLAN table.

Table 35-2 Command Summary: sys sw

COMMAND			DESCRIPTION
	status		Shows the IEEE 802.1Q tagged status.
rstp			All “sys sw rstp” commands relate to rapid STP configuration. Refer to IEEE Std 802.1w. Use “config save” to save your configuration changes.
	bridge	enable	Enables RSTP.
		disable	Disables RSTP.
		priority <priority>	Sets the system priority.
		maxage <Max_Age>	Sets the max age timer
		hellotime <Hello_Time>	Sets the hello timer.
		forwardDelay <Forward_Delay_Time>	Sets the forward delay time
		version <STP:0|RSTP:2>	Displays/enables the STP mode; STP or RSTP. RSTP is the default used when configuring STP via web configurator.
	port	enable <port_no>	Enables RSTP on this port.
		disable <port_no>	Disables RSTP on this port.
		pathCost <Port_NO> <Cost|0:Auto>	Sets the specified port’s path cost.
		priority <Port_NO> <Priority>	Sets the specified port’s priority.
		edgeport <port_no>	Displays if this port is an edge port.
		p2pLink <Port_NO> <Auto:2|True:1|False:0>	Sets the specified port can connect to one bridge or multiple bridges.
		mcheck <Port_NO>	Enables the Port Protocol Migration state machine (Disabled, Blocking, Listening, Learning, Forwarding) on the specified port.
lacp			Refer to IEEE 802.3ad for more information on link aggregation control protocol.
	agg		Displays ports trunked using LACP.
	port	enable <port_no>	Enables LACP on the specified port.
		disable <port_no>	Disables LACP on the specified port.
		status <port_no>	Displays whether LACP is enabled on the specified port.

Table 35-2 Command Summary: sys sw

COMMAND			DESCRIPTION
		actoradm activity [port_no] [0:passive 1:active]	Allows/disallows the specified local port to engage in trunking.
		actoradm display [port_no]	Shows whether the specified local port is engaged in trunking.
		actoradm key [port_no][key]	Shows the specified local port LACP key.
		actoradm priority [port_no] [priority]	Sets the specified local port LACP priority.
		actoradm timeout [port_no] [0:long_timeout|1:short_timeout]	Enables a short or long timeout on the specified local port.
	status	<Port_NO>	Displays LACP status on a port.
	keymgnt	[on|off]	Turns LACP key management on or off.
	syspriority	<priority>	Sets the LACP system priority. The switch with the lowest priority becomes the LACP “server”.
	trace		Sets the LACP debug level.
dot1x			“sys sw dot1x” commands relate to IEEE 802.1X security.
	enable		Enables 802.1X security on the switch.
	disable		Disables 802.1X security on the switch.
	status		Shows switch 802.1X security status.
	port		
		enable <port_no>	Enables 802.1X security on the specified port.
		disable <port_no>	Disables 802.1X security on the specified port.
		reauth <port_no> <on|off>	Turns re-authentication on or off on the specified port.
		period <port_no><value>	Configures how often the specified port should be re-authenticated.
		status <port_no>	Displays 802.1X security status on the specified port.
	set	auth <profile | radius>	Sets whether an external RADIUS server or the internal switch user database performs authentication.
		control <port-no> <auto |auth | unauth>	Sets how the specified port should be authenticated.

Table 35-2 Command Summary: sys sw

COMMAND			DESCRIPTION
		radius server <ip>	Sets the external RADIUS server IP address.
		radius secret <secret>	Sets the external RADIUS server password.
		radius port <port>	Sets the external RADIUS server port number.
		radius show	Displays the external RADIUS server settings.
		profile	Internal switch user database. Information in this database is flushed on restarting the switch.
		add <username> <passwd>	Creates a username and password profile in the internal switch user database.
		delete <idx>	Deletes a username and password profile in the internal switch user database.
		list	Lists all profiles in the internal switch user database.
class			A class is the basic rule parameters for a bandwidth control, port mirror or port filter rule.
	display		Displays run-time bandwidth control, port mirror and port filter rule status.
	l2find	<src port> <src MAC> <src vid> <dest port> <dest MAC> <dest vid> <protocol>	Find source/destination port, MAC address and VLAN group information.
	l2set	<src port> <src mac> <src vid><dest port><dest mac> <dest vid>	Sets L2 class rule.
	l3set	<src ip/mask_bits><dest ip/mask_bits> <protocol>	Sets L3 class rule.
	l4set	<src ip/mask_bits> <dest ip/mask_bits> <protocol> <src port> <dest port>	Sets L4 class rule.
	del	<Class Idx>	A class is automatically created when you create a bandwidth control, port mirror or port filter rule. This command deletes the specified class.
	vlanset	<src vid> <dest vid> <protocol>	Sets VLAN class.
bmstorm			These commands relate to broadcast storm control.

Table 35-2 Command Summary: sys sw

COMMAND			DESCRIPTION
	disable		Clears current run-time settings
	type	<dir (ingress/egress)> <type (broadcast/multicast/both)>	Specifies the type of frames to limit in the switch; broadcast, multicast or both.
	display	[index]	Displays broadcast storm control ports' settings
	interval	[value]	Sets/displays the monitor interval.
	set	<port><threshold><direction>	Specifies the packet threshold and direction (ingress/egress) on the specified port.
	del	<index>	Disables broadcast storm control on this port.
mac	static		Displays static MAC addresses.
		disable	Clears current run-time static MAC address settings
		display [<mac> <vid>]	Displays current run-time static MAC addresses on the ports.
		set <port> <MAC> <vid>	Configures a static MAC address on the specified port.
		del <port> <MAC> <vid>	Deletes a static MAC address on the specified port.
	ageSet	<timeout>	Sets aging timeout.
	ageView		Displays the aging timeout period.
filter			The following commands relate to port filters. Port filtering means sifting traffic from one or all ports to one or all ports based on the source and/or destination MAC addresses and VLAN group.
	applyidx	<class index>	Apply class to a filter.
	del	<Class Idx>	Deletes filter class.
	disable		Clears current run-time filters.
	display		Displays current run-time filter status.
	l2set	<src port><src mac><src vid><dest port><dest mac><dest vid>	Creates a filter rule using source/destination port, MAC address and VLAN group information. "*" means "any".
mirror			The following commands relate to port mirrors. Port mirroring is copying traffic from one or all ports to another or all ports for external analysis.

Table 35-2 Command Summary: sys sw

COMMAND			DESCRIPTION
	applyidx	<Class Idx> <MirrorType=input|output|both>	Applies class to mirroring.
	del	<Class Idx>	Deletes a mirroring class.
	disable		Clears current run-time port mirror settings.
	display	[class idx]	Displays current run-time port mirror settings.
	set	<src port> <src MAC> <src vid> <dest port> <dest MAC> <dest vid>	Creates a mirror rule using source/destination port, MAC address and VLAN group information. “*” means “any”.
		<input|output|both>	Sets the direction of mirrored traffic.
	port	<port>	Sets the mirror port (the port traffic is copied to for analysis).
bw			The following commands relate to bandwidth control rules. Bandwidth control means defining a maximum allowable bandwidth for traffic flows from specified source(s) to specified destination(s).
	applyidx	<Class Idx> <Max BW>	Apply class to bandwidth control.
	del	<Class Idx>	Delete a bandwidth control class.
	disable		Clears current run-time bandwidth control rules.
	display		Displays current run-time bandwidth control rules.
	set	<src port><src mac><src vid><dest port><dest mac><dest vid><max bw>	Creates a bandwidth control rule using source/destination port, MAC address and VLAN group information. “*” means “any”.
trunk			The following commands relate to trunking. Trunking is the grouping of physical ports into one logical higher-capacity link.
	del	<id>	Deletes a trunk group.
	disable		Clears current run-time trunk settings.
	display		Displays current run-time trunk settings.
	listView		Displays member list of trunk.
	set	<group><# ports>	Adds ports to a trunk group.

Table 35-2 Command Summary: sys sw

COMMAND			DESCRIPTION
ingress	set	<port> <enable | disable>	Sets ingress check on a port.
	get	<port>	Gets ingress check state on a port.
	viewAll		Gets ingress check state on all ports.
learn	enable	[port]	Enables address learning on the port.
	disable	[port]	Disables address learning on the port.
	display	[port]	Displays address learning status.
isolate	disable		Disables port isolation.(All connected)
	port	<port> <Port-List (in Hex)>	Sets the port-list which can connect to the specific port.
	enable		Enables port isolation.
mc	set	<addr> <port>...	Sets ports to a specific multicast address
	del	<addr>	Deletes a specific multicast address
	get	<addr>	Shows settings of the multicast address
vlan	status		Displays VLAN status
	type	<802.1q | port-based>	Sets VLAN mode
diffserv	enable		Enables diffserv
	disable		Disables diffserv
	defdscp	<DSCP (Hex)>	Sets the default DSCP of the diffserv
	portdefdscp	<port> <on/off>	Sets the status of default DSCP for this port <port>
	mark	<class idx> <DSCP (Hex)>	Applies class to diffserv
	del	<class idx>	Deletes diffserv class
	disp		Displays current diffserv status
	queue	<DSCP (Hex)> <queue>	Maps a particular DSCP to a queue
	priority	<DSCP (Hex)> <priority>	Maps a particular DSCP to a 802.1p priority
	precedence	<DSCP (Hex)> <precedence (Hex)>	Maps a particular DSCP to a precedence

35.2.3 EXIT Command

Table 35-3 CLI Command Summary: EXIT

COMMAND	DESCRIPTION
Exit	Ends the console or telnet session.

35.2.4 ip Commands

Table 35-4 Command Summary: ip

COMMAND			DESCRIPTION
ip	address	[addr]	Displays the host IP address.
	alias	<iface>	Sets an alias for the specified interface.
	aliasdis	<0|1>	Disables/enables the alias for the specified interface.
	arp	status	Displays all interfaces' IP Address Resolution Protocol status.
		add <hostid> ether <ether addr>	Adds a static ARP entry.
		drop [hostid][arpType]	Deletes a static ARP entry.
		flush	Flushes the ARP table.
	dhcp<vid>	Mode <server>|<relay>|<none>	Sets the DHCP mode.
		Server netmask <netmask>	Sets the subnet mask for the DHCP server.
		Server gateway <gatewayIP>	Sets gateway for the DHCP server.
		Server pool <startIP> <numIP>	Sets the starting client IP address and pool for the DHCP server.
		Server reset	Resets the DHCP server.
		server hostname <hostname>	Sets the hostname for the DHCP server.
		server dnsserver <dnsIP1> [<dnsIP2>] [dnsIP3]	Sets the DNS server for the DHCP server.
		server winsserver <winsIP1> [<winsIP2>]	Set the WINS server for the DHCP server.
		relay server <serverIP1> [serverIP2] [serverIP3]	Sets the DHCP relay server(s).
		Status	Displays DHCP status.
	dhcpconfig	Add <vid>	Adds DHCP configuration for the VID.
		del<vid>	Deletes DHCP configuration for the VID.
		disp	Shows DHCP configuration.
	dvmrp	enable	Enables DVMRP.

Table 35-4 Command Summary: ip

COMMAND			DESCRIPTION
		disable	Disables DVMRP.
		Iface <iface> enable	Enables DVMRP on the interface.
		Iface <iface> disable	Disables DVMRP on the interface.
		Iface <iface> ttl <ttlvalue>	Sets TTL threshold value for the interface.
		route	Displays DVMRP routing table.
		prune	Displays DVMRP prune table.
		group	Displays DVMRP group table.
		interface	Displays DVMRP interface table.
		neighbor	Displays DVMRP neighbors.
	httpd	debug [on|off]	Enables or disables the HTTP debug flag.
	icmp		
		status	Displays the ICMP statistics counter.
		discovery <iface> [on|off]	Sets the ICMP router discovery flag.
	ifconfig	[iface] [ipaddr] [broadcast <addr> |mtu <value>|dynamic]	Configures a network interface.
	igmpsnoop	status	Displays the IGMP group table.
		querier	Displays the port number of the incoming port that received the latest IGMP querier.
		enable	Turns on IGMP snooping.
		disable	Turns off IGMP snooping.
	igmp	debug	Sets IGMP debug level
		forwardall	Activates/deactivates IGMP forwarding to all interfaces flag
		querier	Turns on/off IGMP stop query flag
		iface <iface>	Sets/shows IGMP related parameters for the interface
		robustness	Sets IGMP robustness variable
		status	Displays IGMP run-time status.
	ospf	Enable	Activates OSPF.
		Disable	Deactivates OSPF.
		abr-type <cisco|ibm|shortcut|standard>	Sets the area border router (ABR) type.

Table 35-4 Command Summary: ip

COMMAND			DESCRIPTION
		auto-cost reference-bandwidth <1-4294967>	Sets the cost associated to the interface. The ES calculates the cost based on the reference bandwidth.
		default-metric <0-16777214>	Sets the default metric value
		neighbor A.B.C.D [priority <0-255>] [poll-interval <1-65535>]	Adds a neighbor.
		network A.B.C.D/M area [A.B.C.D|<0-4294967295>]	Adds a network to an area.
		passive-if <iface> [A.B.C.D]	Sets an interface to passive. A passive interface does not receive/send packets.
		redistribute [rip|bgp|static] [metric-type 1|2] | [metric <0-16777214>]	Sets OSPF to import/export routes to other routing protocols.
		refresh timer <10-1800>	Sets the time (in seconds) to update OSPF information.
		rfc1583	
		router-id <A.B.C.D>	Sets the router ID.
		timers spf <0-4294967295 (Delay Timer)> <0-4294967295 (Hold Timer)>	Sets the delay and hold timers.
		area auth <0-4294967295|A.B.C.D> <none|simple|md>	Sets the authentication method of an area.
		area default-cost <0-4294967295|A.B.C.D> <0-16777215>	Sets the default cost of an area.
		area stub <0-4294967295|A.B.C.D> [no-summary]	Sets an area as a stub area.
		area virtual-link <0-4294967295|A.B.C.D> A.B.C.D [...]	Adds a virtual link(s) to an area.
		area clear auth <0-4294967295|A.B.C.D>	Erases the authentication settings of an area.
		area clear default-cost <0-4294967295>|A.B.C.D) <0-16777215>	Erases the default cost of an area.
		area clear stub <0-4294967295>|A.B.C.D> [no-summary]	Erases the stub settings of an area.
		area clear virtual-link <0-4294967295|A.B.C.D> A.B.C.D [...]	Erases the virtual link settings of an area.
		iface auth <iface> [none|simple|md] [A.B.C.D]	Sets the authentication method of an interface.
		iface cost <iface> <1-65535> [A.B.C.D]	Sets the cost of an interface.

Table 35-4 Command Summary: ip

COMMAND			DESCRIPTION
		iface dead-interval <iface> <1-65535> [A.B.C.D]	Sets the dead interface of an interface.
		iface desc <iface> LINE	
		iface hello-interval <iface> <1-65535> [A.B.C.D]	Sets the hello time interval on an interface.
		iface md-key <iface> <1-255> md5 KEY [A.B.C.D]	Sets the MD5 authentication key.
		iface network <iface> <broadcast|non-broadcast|point-to-multipoint|point-to-point>	Sets the network type of an interface.
		iface priority <iface> <0-255> [A.B.C.D]	Sets the priority of an interface.
		iface retx-interval <iface> <3-65535> [A.B.C.D]	Sets the retransmission time interface on an interface.
		iface simple-key <iface> SIMPLE_KEY [A.B.C.D]	Sets the simple authentication key.
		iface status <iface>	Displays the status of an interface.
		iface tx-delay <iface> <1-65535> [A.B.C.D]	Sets the transmission delay timer on an interface.
		iface clear auth <iface> [A.B.C.D]	Erases the authentication settings of an interface.
		iface clear cost <iface> [A.B.C.D]	Erases the cost setting of an interface.
		iface clear dead-interval <iface> [A.B.C.D]	Erases the dead interface of an interface.
		iface clear desc <iface>	
		iface clear hello-interval <iface> [A.B.C.D]	Erases the hello time interval on an interface.
		iface clear md-key <iface> <1-255> [A.B.C.D]	Erases the MD5 authentication key.
		iface clear network <iface>	Erases the network type of an interface.
		iface clear priority <iface> [A.B.C.D]	Erases the priority of an interface.
		iface clear retx-interval <iface> [A.B.C.D]	Erases the retransmission time interface on an interface.
		iface clear simple-key <iface> [A.B.C.D]	Erases the simple authentication key.
		iface clear tx-delay <iface> [A.B.C.D]	Erases the transmission delay timer on an interface.
		status database	Displays the link state database.
		status interface	Displays the interface status.

Table 35-4 Command Summary: ip

COMMAND			DESCRIPTION
		status memory	Displays the sizes of the buffers.
		status neighbor	Displays the neighbor information.
		status route	Displays the OSPF routing tables.
		log list	Lists the log levels.
		log level [mask]	Sets the log level.
		clear abr-type <cisco|ibm|shortcut>	Clears the area border router (ABR) type.
		clear auto-cost	Clears the cost associated to the interface. The ES calculates the cost based on the reference bandwidth.
		clear default-metric	Clears the default metric of the interface.
		clear neighbor A.B.C.D [priority <0-255>] [poll-interval <1-65535>]	Removes a neighbor.
		clear network <A.B.C.D/M> area <A.B.C.D|0-4294967295>	Removes a network to an area.
		clear passive-if <iface> [A.B.C.D]	Clears the passive setting on an interface. A passive interface does not receive/send packets.
		clear redistribute <rip|bgp|static>	Sets OSPF not to import/export routes to other routing protocols.
		clear refresh timer [10-1800]	Resets the time (in seconds) to update OSPF information.
		clear rfc1583	
		clear router-id	Erases the router ID.
		clear timers	Resets the delay and hold timers.
	ping	<hostid>	Pings a remote host.
	route	status	Displays the routing table.
		add <dest addr>[/<bits>] <gateway> [<metric>]	Adds a route.
		addiface <dest addr>[/<bits>] <iface> [<metric>]	Adds an entry to the routing table for the specified interface.
		addprivate <dest addr>[/<bits>] <gateway> [<metric>]	Adds a private route.
		drop <host addr> [/<bits>]	Drops a route.
	rtDomain	add <ip> <netmask> <vid> [save:0|1] [name]	Adds a routing domain
		del <index> [save:0|1]	Deletes a routing domain.
		display	Shows current rout domain status

Table 35-4 Command Summary: ip

COMMAND			DESCRIPTION
	set_igmp_mode	<mode>	Sets mode as IGMP (1) or IGMP snooping(2).
	status		Displays IP statistic counters.
	tcp	ceiling [value]	Sets the TCP maximum round trip time.
		floor [value]	Sets the TCP minimum round trip time.
		irtt [value]	Sets the TCP default initial round trip time.
		kick <tcb>	Drops the TCP connection of the specified TCP Control Block (TCB).
		limit [value]	Sets a TCP output window limit.
		mss [value]	Inputs the TCP Maximum Segment Size.
		reset <tcb>	Resets the TCP connection of the specified TCP Control Block (TCB).
		rtt <tcb> <value>	Sets the round trip time for the TCP control block.
		status [tcb] [<interval>]	Displays the TCP statistic counters.
		syndata [on|off]	Turns on/off the option to send data with the SYN packet.
		trace [on|off]	Turns on/off the trace for debugging.
	telnet	<host> [port]	Telnets to the specified host.
	traceroute	<host> [ttl] [wait] [queries]	Sends ICMP packets to trace the route of a remote host.
	udp	status	Displays the UDP status.

35.2.5 config Command

Table 35-5 Command Summary: config

COMMAND		DESCRIPTION
config	save	You can use the “config save” command to save 802.1Q, STP, Cluster and IP configuration changes to non-volatile memory (Flash). These changes are effective after you restart the switch. However you cannot use “config save” for all other line command configurations. These are saved in volatile memory (DRAM), so are not effective after you restart the switch.

Chapter 36
Command Examples

This chapter describes some commands in more detail.

36.1 Commonly Used Commands Overview

These are commands that you may use frequently in configuring and maintaining your switch. See the following chapter for IEEE 802.1Q Tagged VLAN commands.

36.2 sys Commands

These are the commonly used commands that belong to the sys (system) group of commands.

36.2.1 sys log disp

Syntax:

```
sys log disp
```

This command displays the system error log. An example is shown next.

```
ras> sys log disp
   1 Wed Feb 12 15:27:45 2003 PP1d  ERROR unknown variable
   6 Wed Feb 12 15:34:42 2003 PP13  INFO  SMT Password pass
   9 Wed Feb 12 16:16:46 2003 PP13  INFO  SMT Password pass
  11 Wed Feb 12 16:26:06 2003 PP1d  ERROR unknown variable
  12 Wed Feb 12 16:31:18 2003 PP13  INFO  SMT Password pass
  14 Wed Feb 12 16:42:20 2003 PP13  INFO  SMT Password pass
  16 Wed Feb 12 16:55:39 2003 PP13  INFO  SMT Password pass
  18 Wed Feb 12 17:19:30 2003 PP13  INFO  SMT Password pass
  20 Wed Feb 12 17:43:31 2003 PP13  INFO  SMT Password pass
  22 Wed Feb 12 17:45:48 2003 PP1d  ERROR unknown variable
  23 Thu Feb 13 09:08:09 2003 PP14  ERROR Last errorlog repeat 54 Times
  26 Thu Feb 13 09:23:53 2003 PP13  INFO  SMT Password pass
  28 Thu Feb 13 09:36:05 2003 PP13  INFO  SMT Password pass
  30 Thu Feb 13 09:52:48 2003 PP13  INFO  SMT Password pass
  34 Thu Feb 13 10:32:02 2003 PP13  INFO  SMT Password pass
  36 Thu Feb 13 11:51:02 2003 PP1f  INFO  adjtime task pause 1 day
  37 Thu Feb 13 12:06:22 2003 PP13  INFO  SMT Password pass
  39 Thu Feb 13 12:15:12 2003 PP13  INFO  SMT Password pass
  42 Thu Feb 13 16:17:25 2003 PP13  INFO  SMT Password pass
```

Figure 36-1 sys log disp Command Example

36.2.2 sys log clear

Syntax:

```
sys log clear
```

This command clears the system error log.

If you clear a log (using the `sys log clear` command), you cannot view it again.

36.2.3 sys version

Syntax:

```
sys version
```

This command shows the RAS code, firmware version, system uptime and bootbase version.

An example is shown next.

```
ES-4024> sys version
ZyNOS version: V3.50(DU.0)b8 | 08/18/2003
romRasSize: 1513458
system up time:     0:03:37 (550d ticks)
bootbase version: V1.0 | 04/25/2003
```

Figure 36-2 sys version Command Example

36.2.4 sys monitor status

Syntax:

```
sys monitor status
```

This command shows the hardware monitor's status.

An example is shown next.

```
ES-4024> sys monitor status
   Time      V0     V1     V2     V3     V4     T0    T1    T2   F00   F01   F02   F10   Error
---------- ------ ------ ------ ------ ------ ----- ----- ----- ----- ----- ----- ----- --------
      345   2.512  1.840  3.296 12.160  4.992  33.0  32.0  32.0  5882  6010  5967  5841 00000000
```

Figure 36-3 sys monitor status Command Example

36.2.5 sys sw vlan1q vlan list

Syntax:

```
sys sw vlan1q vlan list <all|VID|start_VID|end_VID>
```

where

`<all|VID|start_VID|end_VID>=`	Specify either all of the VLAN entries (`all`), a single VLAN ID (`VID`) or a range of VLAN IDs starting from a certain VID (`start_VID`) or a range of VLAN Ids ending at a specific VID (`end_VID`).

This command displays the IEEE 802.1Q tagged VLAN table. An example is shown next.

```
ES-4024> sys sw vlan1q vlan list all

   No.   VID  ElapsedTime  Status  EgressPort/UntaggedPort
  ------ ---- -----------  ------  -------------------------------
    1)     1      0:39:52  Static  EEEEE|EEEEE|EEEEE|EEEEE|EEEEE|EEE
                                   UUUUU|UUUUU|UUUUU|UUUUU|UUUUU|UUU
```

Figure 36-4 sys sw vlan1q vlan list Command Example

36.2.6 sys ixe2424 pktcnt

Syntax:

```
sys ixe2424 pktcnt <port 1-28>
```

This command displays statistics of a port. An example is shown next.

```
ES-4024> sys ixe2424 pktcnt 2
          DropEvents:          0
              Octets:     340532
                Pkts:       2053
       BroadcastPkts:        263
       MulticastPkts:        174
      CRCAlignErrors:          0
       UndersizePkts:          0
        OversizePkts:          0
           Fragments:          0
             Jabbers:          0
          Collisions:          0
        Pkts64Octets:        739
   Pkts65to127Octets:        182
  Pkts128to255Octets:        196
  Pkts256to511Octets:         32
 Pkts512to1023Octets:         16
Pkts1024to1518Octets:          0
              TxPkts:        888
     TxMulticastPkts:          0
     TxBroadcastPkts:         16
         TxPausePkts:          0
              RxPkts:       1165
     RxMulticastPkts:        174
     RxBroadcastPkts:        247
         RxPausePkts:          0
           Alignment:          0
       LateCollision:          0
  ExcessiveCollision:          0
     SingleCollision:          0
   MultipleCollision:          0
             TxBytes:     216431
             RxBytes:     124101
     RxCodeViolation:          0
        RxRangeError:       1046
           RxControl:          0
         RxVLANFrame:          0
          RxRuntPkts:          0
               RxBig:          0
               RxCRC:          0
               TxCRC:          0
            TxDefer:          0
          TxControl:          0
         TxVLANFrame:          0
```

Figure 36-5 sys ixe2424 pktcnt Command Example

36.2.7 sys ixe2424 dbm ip list

Syntax:

```
sys ixe2424 dbm ip list
```

This command displays the IP address(es) stored on the system chip (ixe2424). An example is shown next.

```
ES-4024> sys ixe2424 dbm ip list
        Status VlanId    IPAddr      Port
       Static      1       10.1.1.1  CPU
       Static      0 10.255.255.255 CPU
       Static      1    192.168.1.1 CPU
      Dynamic      1   192.168.1.10   2
       Static      0  192.168.1.255 CPU
```

Figure 36-6 sys ixe2424 dbm ip list Command Example

36.2.8 sys ixe2424 dbm mac list

Syntax:

```
sys ixe2424 dbm mac list
```

This command displays the MAC address(es) stored on the system chip (ixe2424). An example is shown next.

```
ES-4024> sys ixe2424 dbm mac list
 Port    VlanTag         MacAddres
 2       1              00:50:ba:ad:4f:81
 6       1              00:a0:cf:41:f0:06
```

Figure 36-7 sys ixe2424 dbm mac list Command Example

36.3ipCommands

These are the commonly used commands that belong to the ip group of commands.

36.3.1 ip ping

Syntax:

```
ip ping <hostid>
```

This command pings a remote host. An example is shown next.

```
ES-4024> ip ping 192.168.1.10
Resolving 192.168.1.10... 192.168.1.10
      sent      rcvd  rate    rtt     avg    mdev     max     min
         1         1  100       0       0       0       0       0
         2         2  100       0       0       0       0       0
         3         3  100       0       0       0       0       0
```

Figure 36-8 ip ping Command Example

36.3.2 ip route status

Syntax:

```
ip route status
```

This command displays the routing table. An example is shown next.

```
ES-4024> ip route status

Dest            FF Len Device     Gateway         Metric stat Timer  Use
192.168.1.0     00 24  swp00      192.168.1.1       1    041b 0      3
default         00 0   swp00      192.168.1.254     2    001b 0      4205
```

Figure 36-9 ip route status Command Example

36.3.3 ip rtDomain display

Syntax:

```
ip rtDomain display
```

This command displays the IP routing table. An example is shown next.

```
ES-4024> ip rtDomain display

swif0: mtu 1500  ,Index 0
    inet 0.0.0.0, netmask 0x00000000, broadcast 0.0.0.0
    RIP RX:None, TX:None, VID:   0
swif1: mtu 1500  ,Index 1
    inet 192.168.1.1, netmask 0xffffff00, broadcast 192.168.1.255
    RIP RX:None, TX:None, VID:   1
swif2: mtu 1500  ,Index 2
    inet 10.1.1.1, netmask 0xff000000, broadcast 10.255.255.255
    RIP RX:None, TX:None, VID:   1
```

Figure 36-10 ip rtDomain display Command Example

36.3.4 ip rtDomain add

Syntax:

```
ip rtDomain add <ip> <netmask> <vid>
```

This command adds a new IP routing domain. An example is shown next.

```
ES-4024> ip rtDomain add 10.1.1.1 255.0.0.0 1
```

Figure 36-11 ip rtDomain add Command Example

36.3.5 ip rtDomain delete

Syntax:

```
ip rtDomain delete <ip> <netmask>
```

This command removes an IP routing domain. An example is shown next.

```
ES-4024> ip rtDomain delete 10.1.1.1 255.0.0.0
```

Figure 36-12 ip rtDomain delete Command Example

36.3.6 ip arp status

Syntax:

```
ip arp status
```

This command displays all interfaces' IP Address Resolution Protocol (ARP) status. An example is shown next.

```
ES-4024> ip arp status

received 1 badtype 0 bogus addr 0 reqst in 0 replies 1 reqst out 4 bad VID 0
cache hit 29 (0%), cache miss 8366 (99%)
IP-addr         Type           Time  Addr              stat iface channel
192.168.1.1     Ethernet       0     00:a0:c5:3f:91:56 43   NULL  NULL
num of arp entries= 1
```

Figure 36-13 ip arp status Command Example

36.3.7 Enabling RSTP on the Stacking Module

Step 1. First enable RSTP

```
sys sw rstp bridge enable
```

Step 2. Then enable RSTP on the stacking port.

```
sys sw rstp port enable S1
sys sw rstp port enable S2
```

Step 3. Save the configuration

```
config save
```

Chapter 37
IEEE 802.1Q Tagged VLAN

This chapter describes the IEEE 802.1Q Tagged VLAN and associated commands. Use the "config save" command to save configuration changes.

37.1IEEE 802.1Q Tagged VLAN Overview

See the *VLAN* chapter for more information on VLANs. There are two kinds of tagging:

1. Explicit Tagging

A VLAN identifier is added to the frame header that identifies the source VLAN.

2. Implicit Tagging

The MAC (Media Access Control) number, the port or other information is used to identify the source of a VLAN frame.

The IEEE 802.1Q Tagged VLAN uses both explicit and implicit tagging.

It is important for the switch to determine what devices are VLAN-aware and VLAN-unaware so that it can decide whether to forward a tagged frame (to a VLAN-aware device) or first strip the tag from a frame and then forward it (to a VLAN-unaware device).

37.2Filtering Databases

A filtering database stores and organizes VLAN registration information useful for switching frames to and from a switch. A filtering database consists of a static entries (Static VLAN or SVLAN table) and dynamic entries (Dynamic VLAN or DVLAN table).

37.2.1 Static Entries (SVLAN Table)

Static entry registration information is added, modified and removed by administrators only.

37.2.2 Dynamic Entries (DVLAN Table)

Dynamic entries are learned by the switch and cannot be created or updated by administrators. The switch learns this information by observing what port, source address and VLAN ID (or VID) is associated with a frame. Entries are added and deleted using GARP VLAN Registration Protocol (GVRP), where GARP is the Generic Attribute Registration Protocol.

37.3Configuring Tagged VLAN

The following procedure shows you how to configure tagged VLAN.

Step 1. Use the IEEE 802.1Q tagged VLAN commands to configure tagged VLAN for the switch.

- Use the `sys sw vlan1q svlan setentry` command to configure a VLAN ID for each port on the switch.
- Use the `sys sw vlan1q svlan active` command when you are finished configuring the VLAN (see the last step).
- Use the `sys sw vlan1q port defaultVID command` to set the VLAN ID you created for a port to that specific port in the PVID table.
- Use the `sys sw vlan1q svlan active` command to activate the VLAN IDs.

Example:

```
ES-4024> sys sw vlan1q svlan setentry up1 2000 24 fixed tag
for newly create VLAN, please use svlan active <VID> to activate this entry

ES-4024> sys sw vlan1q port defaultVID 24 2000

ES-4024> sys sw vlan1q svlan setentry up1 2001 25 fixed untag

for newly create VLAN, please use svlan active <VID> to activate this entry
ES-4024> sys sw vlan1q port defaultVID 25 2001

ES-4024> sys sw vlan1q svlan active 2000

ES-4024> sys sw vlan1q svlan active 2001
```

Figure 37-1 Tagged VLAN Configuration and Activation Example

Step 2. Configure your management VLAN.

- Use the `sys sw vlan1q svlan setentry` command to configure a VLAN ID (VID 3 in this example) for managing the switch (the “management” or “CPU” VLAN).
- Use the `sys sw vlan1q svlan active` command to activate the new management VLAN ID.

Example:

```
ES-4024> sys sw vlan1q svlan setentry example 3 24 fixed tag

ES-4024> sys sw vlan1q svlan active 3
```

Figure 37-2 CPU VLAN Configuration and Activation Example

Step 3. Perform the procedure below to complete the VLAN setup.

a. Telnet to the operational IP address of the switch.

b. Use the `sys sw vlan1q svlan cpu` command to set VID 3 as the management VLAN.

c. Use the `sys sw svlan delentry` command to remove the default VLAN ID (1).

Example:

```
ES-4024> sys sw vlan1q svlan cpu 3
ES-4024> sys sw vlan1q svlan delentry 1
```

Figure 37-3 Deleting Default VLAN Example

37.4IEEE VLAN1Q Tagged VLAN Configuration Commands

These `sw` (switch) commands allow you to configure and monitor the IEEE 802.1Q Tagged VLAN.

37.4.1 sys sw garp status

Syntax:

```
sys sw garp status
```

This command shows the switch's GARP timer settings, including the join, leave and leave all timers.

An example is shown next.

```
ES-4024> sys sw garp status

GARP Timer Status :
        Join Timer = 200 msec
        Leave Timer = 600 msec
        Leave All Timer = 10000 msec
ES-4024>
```

Figure 37-4 sys sw garp status Command Example

37.4.2 sys sw garp timer

Syntax:

```
sys sw garp timer<join timer(ms)> <leave timer(ms)> <leave all
timer<ms>
```

where

`<join timer (ms)>`	=	This sets the duration of the Join Period timer for GVRP in milliseconds. Each port has a Join Period timer. The allowed Join Time range is between 100 and 32767 milliseconds; the default is 200 milliseconds.
`<leave timer(ms)>`	=	This sets the duration of the Leave Period timer for GVRP in milliseconds. Each port has a single Leave Period timer. Leave Time must be two times larger than Join Timer; the default is 600 milliseconds.

`<leave all timer<ms>=`	This sets the duration of the Leave All Period timer for GVRP in milliseconds. Each port has a single Leave All Period timer. Leave All Timer must be larger than Leave Timer; the default is 10000 milliseconds.

This command sets the switch's GARP timer settings, including the join, leave and leave all timers.

Switches join VLANs by making a declaration. A declaration is made by issuing a Join message using GARP. Declarations are withdrawn by issuing a Leave message. A Leave All message terminates all registrations. GARP timers set declaration timeout values.

The following example sets the Join Timer to 300 milliseconds, the Leave Timer to 800 milliseconds and the Leave All Timer to 11000 milliseconds.

```
ES-4024> sys sw garp timer 300 800 11000
```

Figure 37-5 sys sw garp timer Command Example

37.4.3 sys sw gvrp status

Syntax:

```
sys sw gvrp status
```

This command shows the switch's GVRP settings.

An example is shown next.

```
ES-4024> sys sw gvrp status
GVRP control block status:
  gvrpEnable = 1
  gvrpPortEnable:
    OOOOOOOOOOOOOOOOOOOOOOOOXXXX
```

Figure 37-6 sys sw gvrp status Command Example

37.4.4 sys sw gvrp enable

Syntax:

```
sys sw gvrp enable
```

This command turns on GVRP in order to propagate VLAN information beyond the switch.

37.4.5 sys sw gvrp disable

Syntax:

```
sys sw gvrp disable
```

This command turns off GVRP so that the switch does not propagate VLAN information to other switches.

37.4.6 sys sw vlan1q port status

Syntax:

```
sys sw vlan1q port status <port>
```

This command shows information about the specified port's VLAN settings.

The following example shows the settings for port 1.

```
ES-4024> sys sw vlan1q port status 1

Port 1 VLAN Setup :
Default VLAN ID = 1
VLAN Acceptable Type = All
GVRP = DISABLE
Protocol VLAN ID:
  IP : none
  IPX : none
  NETBIOS : none
  APPLETALK : none
```

Figure 37-7 sys sw vlan1q port status Command Example

37.4.7 sys sw vlan1q port defaultVID

Syntax:

```
sys sw vlan1q port defaultVID <port> <VID>
```

where

`<port>` = A port number

`<VID>` = The VLAN ID. Valid parameter range = [1 – 4094].

This command sets a default VLAN ID for all untagged packets that come in through the specified port.

The following example sets the default VID of port 1 to 2000.

```
ES-4024> sys sw vlan1q port defaultVID 1 2000
```

Figure 37-8 sys sw vlan1q port defaultVID Command Example

37.4.8 sys sw vlan1q port accept

Syntax:

```
sys sw vlan1q port accept <port> <all|tagged>
```

where

<port>	=	A port number
<all|tagged>	=	Specifies all Ethernet frames (tagged and untagged) or only tagged Ethernet frames.

This command sets the specified port to accept all Ethernet frames or only those with an IEEE 802.1Q VLAN tag.

The following example sets port 2 to accept only tagged frames.

```
ES-4024> sys sw vlan1q port accept 2 tagged
```

Figure 37-9 sys sw vlan1q port accept Command Example

37.4.9 sys sw vlan1q port gvrp

Syntax:

```
sys sw vlan1q port gvrp <port> <enable|disable>
```

where

<port>	=	A port number
<enable|disable>	=	Turn GVRP on or off.

This command turns GVRP on or off for the specified port.

The following example turns off GVRP for port 2.

```
ES-4024> sys sw vlan1q port gvrp 2 disable
```

Figure 37-10 sys sw vlan1q port gvrp Command Example

37.4.10 sys sw vlan1q svlan cpu

Syntax:

```
sys sw vlan1q svlan cpu <VLAN ID>
```

where

<VID>	=	The VLAN ID. Valid parameter range = [1 – 4094].

This command sets the management VLAN (CPU). You can only use ports that are members of this management VLAN in order to manage the switch.

The following example sets VLAN ID 2 to be the CPU (management) VLAN.

```
ES-4024> sys sw vlan1q svlan cpu 2
```

Figure 37-11 sys sw vlan1q svlan cpu Command Example

37.4.11 sys sw vlan1q svlan setentry

Syntax:

```
sys sw vlan1q svlan setentry <name> <VID> <port> <adctl> <tagctl>
```

where

`<name>`	=	A name to identify the SVLAN entry.
`<VID>`	=	The VLAN ID [1 – 4094].
`<port>`	=	This is the switch port number.
`<adctl>`	=	This is the registrar administration control flag. Valid parameters = [`fixed`, `forbidden`, `normal`]. Enter `fixed` to register a `<port #>` to the static VLAN table with `<vid>`. Enter `normal` to confirm registration of the `<port #>` to the static VLAN table with `<vid>`. Enter `forbidden` to block a `<port #>` from joining the static VLAN table with `<vid>`.
`<tagctl>`	=	This is the tag control flag. Valid parameters = [`tag`|`untag`]. Enter `tag` to tag outgoing frames. Enter `untag` to send outgoing frames without a tag.

This command adds or modifies an entry in the static VLAN table. Display your configuration by using the `sys sw vlan1q svlan list` command. An example of a configuration is shown next.

Modify a Static VLAN Table Example

The following is an example of how to modify a static VLAN table.

```
1.      ras> sys sw vlan1q svlan setentry  2000  1  fixed  tag
2.      ras> sys sw vlan1q svlan setentry  2001  2  fixed  tag
```

Figure 37-12 Modifying the Static VLAN Example

Forwarding Process Example

Tagged Frames

Step 1. First the switch checks the VLAN ID (VID) of tagged frames or assigns temporary VIDs to untagged frames (see *Section 37.4.7*).

Step 2. The switch then checks the VID in a frame's tag against the SVLAN table.

Step 3. The switch notes what the SVLAN table says (that is, the SVLAN tells the switch whether or not to forward a frame and if the forwarded frames should have tags).

Step 4. Then the switch applies the port filter to finish the forwarding decision. This means that frames may be dropped even if the SVLAN says to forward them. Frames might also be dropped if they are sent to a CPE (customer premises equipment) DSL device that does not accept tagged frames.

Untagged Frames

Step 1. An untagged frame comes in from the LAN.

Step 2. The switch checks the PVID table and assigns a temporary VID of 1.

Step 3. The switch ignores the port from which the frame came, because the switch does not send a frame to the port from which it came. The switch also does not forward frames to "forbidden" ports.

Step 4. If after looking at the SVLAN, the switch does not have any ports to which it will send the frame, it won't check the port filter.

37.4.12 sys sw vlan1q svlan delentry

Syntax:

```
sys sw vlan1q svlan delentry <VID>
```

where

<VID> = The VLAN ID [1 – 4094].

This command deletes the specified VLAN ID entry from the static VLAN table

The following example deletes entry 2 in the static VLAN table.

```
ES-4024> sys sw vlan1q svlan delentry 2
```

Figure 37-13 VLAN1Q SVLAN DELENTRY Command Example

37.5sys sw vlan1q svlan active

Syntax:

```
sys sw vlan1q svlan active <VID>
```

This command enables the specified VLAN ID in the SVLAN (Static VLAN) table.

37.6sys sw vlan1q svlan inactive

Syntax:

```
sys sw vlan1q svlan inactive <VID>
```

This command disables the specified VLAN ID in the SVLAN (Static VLAN) table.

37.7sys sw vlan1q svlan list

Syntax:

```
sys sw vlan1q svlan list
```

This command shows the IEEE 802.1Q Tagged SVLAN (Static VLAN) table.

An example is shown next.

For the `AdCtl` section of the last column, "-" is a port set to normal, "x" is a forbidden port and "F" is a fixed port.

For the `TagCtl` section of the last column, "T" is a tagged port, "U" is an untagged port.

```
ES-4024> sys sw vlan1q svlan list

802.1Q VLAN Static Entry:
idx. Name         VID  Active   AdCtl / TagCtl
---- ------------ ---- -------- ------------------------
   0            1    1  active  FFFFFFFFFFFFFFFFFFFFFFFFFF
                                 UUUUUUUUUUUUUUUUUUUUUUUUUU
   1          up1 2000  active  ------------------------F----
                                 TTTTTTTTTTTTTTTTTTTTTTTTTT
   2          up1 2001  active  ------------------------F---
                                 TTTTTTTTTTTTTTTTTTTTTTTUTTT
   3      example    3  active  ------------------------F----
                                 TTTTTTTTTTTTTTTTTTTTTTTTTT
ES-4024>
```

Figure 37-14 sys sw vlan1q svlan list Command Example

37.8sys sw vlan1q vlan list

Syntax:

```
sys sw vlan1q vlan list <all|VID|start_VID|end_VID>
```

where

`<all|VID|start_VID|end_VID>=`	Specify either all of the VLAN entries (`all`), a single VLAN ID (`VID`) or a range of VLAN IDs starting from a certain VID (`start_VID`) or a range of VLAN Ids ending at a specific VID (`end_VID`).

This command shows the current IEEE 802.1Q Tagged VLAN table or a specific part of it.

An example is shown next.

For the `EgressPort` section of the last column, "E" is an egress port for this VLAN, "-" is not an egress port for this VLAN.

The `UntaggedPort` section of the last column displays "-" for a tagged port and "U" for an untagged port.

```
ES-4024> sys sw  vlan1q vlan list all

   No.   VID  ElapsedTime  Status  EgressPort/UntaggedPort
  ------ ---- -----------  ------  -------------------------------
    1)     1      1:04:56  Static  EEEEE|EEEEE|EEEEE|EEEEE|EEEEE|EEE
                                   UUUUU|UUUUU|UUUUU|UUUUU|UUUUU|UUU
    2)     3      0:35:13  Static  -----|-----|-----|-----|---E-|---
                                   -----|-----|-----|-----|-----|---
    3)  2000      0:49:17  Static  -----|-----|-----|-----|---E-|---
                                   -----|-----|-----|-----|-----|---
    4)  2001      0:41:21  Static  -----|-----|-----|-----|----E|---
                                   -----|-----|-----|-----|----U|---
ES-4024>
```

Figure 37-15 sys sw vlan1q vlan list Command Example

37.8.1 sys sw vlan1q vlan status

Syntax:

```
sys sw vlan1q vlan status
```

This command displays the current configuration of the IEEE 802.1Q VLAN.

See the following example shows the default VLAN settings. The default VLAN allows all ports to connect to each other and sets them to send untagged packets.

```
ES-4024> sys sw vlan1q status
802.1Q VLAN Setup :
 GVRP = Enable
 Management VLAN ID = 1
```

Figure 37-16 sys sw vlan1q vlan status Command Example

Part VII

Appendix and Index

This part contains product specification information and an Index.

Appendix A
Product Specifications

These are the ES-4024 product specifications.

Chart A General Product Specifications

Uplink Interface		Two fixed GBIC slots
Stacking Interface		One stacking slot supporting one 1000Base-T module
Subscriber Interface		24 10/100 Base-TX interfaces Auto-negotiation Auto-MDIX Compliant with IEEE 802.3/3u Back pressure flow control for half duplex Flow control for full duplex (IEEE 802.3x) RJ-45 Ethernet cable connector Rate limiting at 1Kbps steps
Layer 2 Features	Bridging	16K MAC addresses Static MAC address filtering (port lock) Broadcast storm control Limited maximum number of MAC addresses per port
	Switching	Switching fabric: 12.8Gbps, non-blocking Max. Frame size: 1522 bytes Forwarding frame: 802.3, 802.1q, Ethernet II, PPPoE Prevent the forwarding of corrupted packets
	STP	802.1d spanning tree protocol 802.1w, rapid reconfiguration to recover network failure
	QoS	802.1p Four priority queues Supports RFC 2475 DiffServ, DSCP to IEEE 802.1p priority mapping
	Security	802.1x port-based authentication
	VLAN	Port-based VLAN setting Tag-based (IEEE 802.1Q) VLAN Number of VLAN: 4K Supports GVRP

Chart A General Product Specifications

	Link aggregation	Supports IEEE 802.3ad; static and dynamic (LACP) port trunking Fast Ethernet: three groups (up to 8 ports for each group) Gigabit: one group Stacking: one group
	Port mirroring	All ports support port mirroring
	Bandwidth control	Supports rate limiting at 1Kbps increment Supports IGMP snooping
Layer 3 Features	IP forwarding	Wire-speed IP forwarding 16K IP address table Filtering based on the source/destination IP address
	Routing protocols	Unicast: RIP-V1/V2, OSPF V2 Multicast: DVMRP, VRRP
	IP services	DHCP server/relay
Layer 4 Features	TCP/UDP port-based filtering Bandwidth management	

Chart B Management Specifications

System Control	Alarm/Status Surveillance Automatic alarm and status report Alarm/event history LED indication for alarm and system status Performance monitoring Line speed Four RMON groups 1, 2, 3, 9 (history, statistics, alarms, and events) for enhanced traffic management, monitoring and analysis Throughput monitoring Transmission of ICMP packets Supports port mirroring and aggregation Spanning tree and IGMP snooping setting Supports MIB community string, community access privilege and trap IP setting Software upgrade and download through FTP/TFTP DHCP server/relay Supports login authorization and security levels (read only and read/write) Provide non-volatile memory for system database storage Keep previous system parameters during re-booting

Chart B Management Specifications

	Self diagnostics FLASH memory DRAM Ethernet ports Clustering (up to 8 switches can be manage by one IP)
Network Management	CLI through console port and telnet RS-232C (DB-9) port for local management Web-based management Status display and event report from web-based management Clustering: up to 8 switches can be manage by one IP Link up/down Power on Restart Fan failure Fan recovery SNMP manageable Trap Trap transmission: at least 1 destination Provide fault, performance, configuration, and security managements HP OpenView interface (version 6.1 and above) RMON: four RMON groups 1, 2, 3, 9 (history, statistics, alarms and events) for enhanced traffic management, monitoring and analysis
MIB	RFC1213 MIB II RFC1493 Bridge MIB RFC1643 Ethernet MIB RFC1757 Four groups of RMON RFC2674 VLAN MIB

Chart C Physical and Environmental Specifications

LEDs	Per switch: S1, S2, PWR, SYS, ALARM Per Ethernet port: LNK/ACT, FDX/COL
Dimension	438 mm (W) x 270 mm (D) x 44.5 mm (H) Standard 19” rack mountable
Weight	3.9Kg
Temperature	Operating: 0 ~ 45˚ C (32˚ F ~ 113˚ F) Storage: -25 ~ 70˚ C

Chart C Physical and Environmental Specifications

Humidity	10 ~ 90% (non-condensing)	
Power Supply	Overload protection AC input：100-240VAC, 50/60Hz, 1.5A Max. DC input：-48VDC－-60VDC, 1.84A Max.	
Safety	North America	UL 60950 CSA C22.2 No. 60950 (Canada)
	European Union	EN60950
EMI	North America	Conducted and Radiated Emission: FCC Part15 B (Class A)
	European Union	Conducted/Radiated Emission: EN55022 (Class A) Current Harmonic: EN61000-3-2 Voltage Fluctuation: EN61000-3-3
EMS (European Union)	Electrostatic Discharge (ESD)	EN 55024/EN 61000-4-2
	Radiated Immunity	EN 55024/EN 61000-4-3
	Electrical Fast Transients/Burst	EN 55024/EN 61000-4-4
	Surge Immunity Requirement	EN 55024/EN 61000-4-5
	RF Injected Current	EN 55024/EN 61000-4-6
	Voltage Dips and Interruptions	EN 55024/EN 61000-4-11

Index

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z